Центр
Управления
Гетерогенными
Инфраструктурами

СМИОК. Инструкция по запуску продукта в демо-зоне

ООО «Клируэй Текнолоджис»

2026

Оглавление

1 Введение

Настоящий документ содержит информацию о процессе установки «Системы мониторинга инфраструктуры открытых ключей — СМИОК», на ОС «Astra Linux 1.8» (далее система), а также инструкцию для доступа к уже готовому демо-стенду. На демо-стенде можно ознакомиться с функциональностью системы и протестировать её возможности.

> ⚠ Для выполнения всех действий требуются права локального администратора (Windows) или root (Linux).

2 Служба поддержки

По всем вопросам, связанных с установкой системы и доступу к демо-стенду, следует обращаться в техническую поддержку к сервисным инженерам. Техническая поддержка работает круглосуточно и доступна по следующим каналам связи:

- Телефон: +7 (495) 142-41-42
- Email: support@clearwayintegration.com

3 Использование демо-стенда системы

3.1 Общая информация

Демо-стенд системы расположен во внутреннем контуре компании. Система развернута в минимальной версии и включает в себя <текст>. Для доступа к демо-стенду необходимо настроить VPN, добавить в доверенные сертификаты и перейти на веб-интерфейс управления системой (см. раздел Вход в веб-интерфейс системы).

3.2 Пререквизиты

Программное обеспечение

VPN-клиент	Cisco AnyConnect Secure Mobility Client https://vpn.clearwayintegration.com
Веб-браузер	Любой современный браузер для доступа к интерфейсам управления
Операционная система	Windows или Linux (поддерживаются Debian/Ubuntu и RHEL/CentOS/Fedora)

Требования к аппаратным ресурсам

CPU	2 ядра
RAM	8 ГБ
HDD	70 ГБ

Учетные записи

	Назначение УЗ	Учетная запись	Пароль
1	VPN Адрес шлюза для VPN: 82.142.150.30	Для подключения по VPN запросите учетные данные администратора у сотрудников технической поддержки.	
2	Портал СМИОК	min-audit	L9qsXUTwJAa8fdP

Сертификаты безопасности

Для корректной работы браузера и отсутствия ошибок SSL на компьютере, который используется для подключения к демо-стенду, необходимо установить следующие сертификаты:

- Root CA Cert (корневой сертификат);
- Sub CA Cert (промежуточный сертификат).

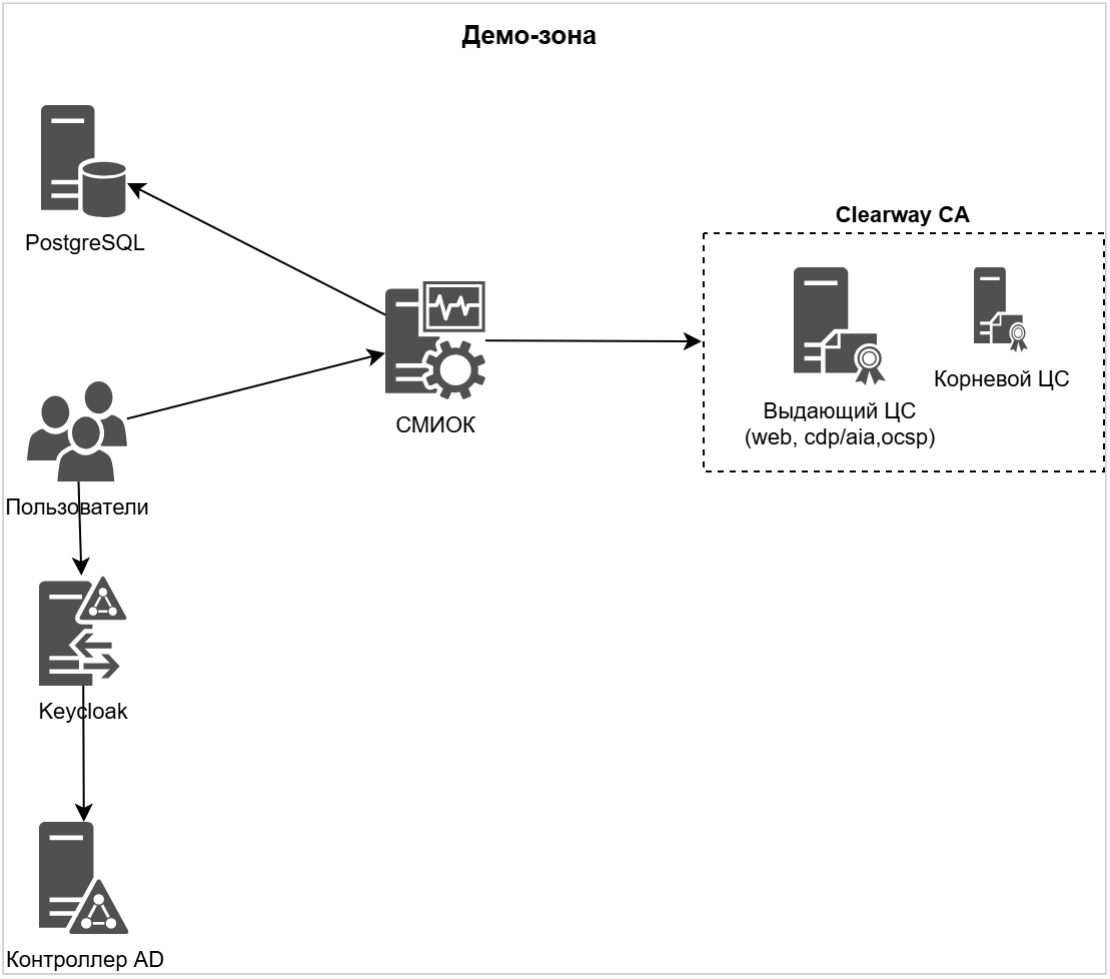
Целевые ресурсы

После настройки доступ осуществляется по адресам:

- Keycloak: https://min-klck.tst.itc.internal.
- Web-интерфейс СМИОК: https://min-smiok.tst.itc.internal.

3.3 Схема развертывания компонентов продукта на демо-стенде

Ниже представлена схема компонентов системы, развернутой по адресу https://min-klck.tst.itc.internal.



1. Хост min-smiok.tst.itc.internal - на этом хосте установлены сервисы СМИОК:

itcagentd	Агент ЦУГИ

nginx	Web-сервер, реверс-прокси, балансировщик
itcsrvd	Мост между агентами и сервером управления
itcdispd	Диспетчер агентов
itcmsgd	Брокер сообщений NATS
ITC.Api.Admin	Сервис для управления настройками сервисов
ITC.Api.CertRkMon	Микросервис отслеживания отозванных сертификатов
ITC.Api.CmdbCore	Обобщённое хранилище сущностей системы
ITC.Api.Collection	Управление коллекциями объектов
ITC.Api.Collreg	Управление реестром коллекций
ITC.Api.CommonCore	Основной сервис Платформы
ITC.Api.CrlMon	Мониторинг списков отзыва (CRL)
ITC.Api.Informer	Сервис управления информерами
ITC.Api.MailOutbox	Отправка почтовых уведомлений
ITC.Api.Pki	Ведение сущностей инфраструктуры открытых ключей

2. Хост min-klck.tst.itc.internal - на этом хосте установлена система управления идентификацией и доступом Keycloak:

KeyCloak 26.0.7	Идентификация и управления доступом

3. Хост min-pgs.tst.itc.internal - на этом хосте установлена СУБД PostgreSQL:

PostgreSQL 15.14	Хранение данных

Список БД для функционирования данного ППО:

itc_pki
itc_pki_certrkmon
itc_pki_collreg
itc_pki_crlmon
itc_pki_mailoutbox

4. Хост min-dc.tst.itc.internal - на этом хосте установлен Контроллер AD:

ActiveDirectory	Служба каталогов

5. Хост min-subca.tst.itc.internal - на этом хосте установлен выдающий центр сертификации.

ClearwayCA	выдающий центр сертификации

3.4 Настройка доступа к демо-стенду

Для настройки доступа к веб-интерфейсу управления системой выполните следующие шаги.

1. Запросите учетные данные для VPN у сотрудников технической поддержки.
2. Авторизуйтесь по VPN.
3. Добавьте в доверенные необходимые сертификаты для ОС Windows / ОС Linux.

3.4.1 Настройка VPN

Доступ во внутренний контур компании обеспечивается с помощью программы Cisco AnyConnect Secure Mobility Client.

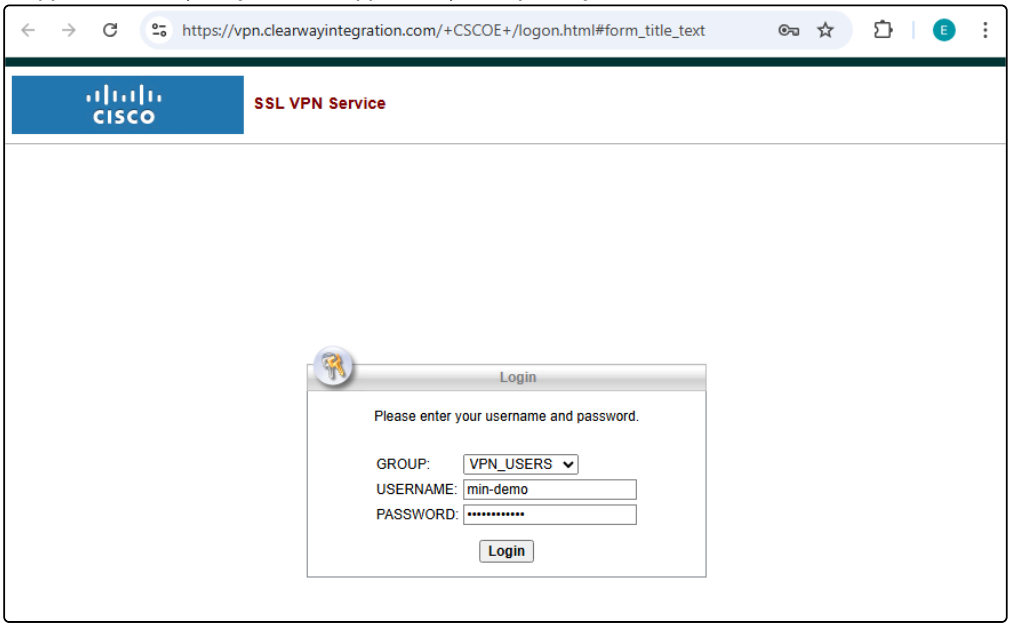
Перед началом установки убедитесь, что:

- вы выполняете инструкцию на рабочем компьютере, на котором будет осуществляться VPN-подключение к ресурсам компании;
- у вас есть права локального Администратора (Windows) или sudo (Linux/macOS);
- отключены другие VPN-соединения.

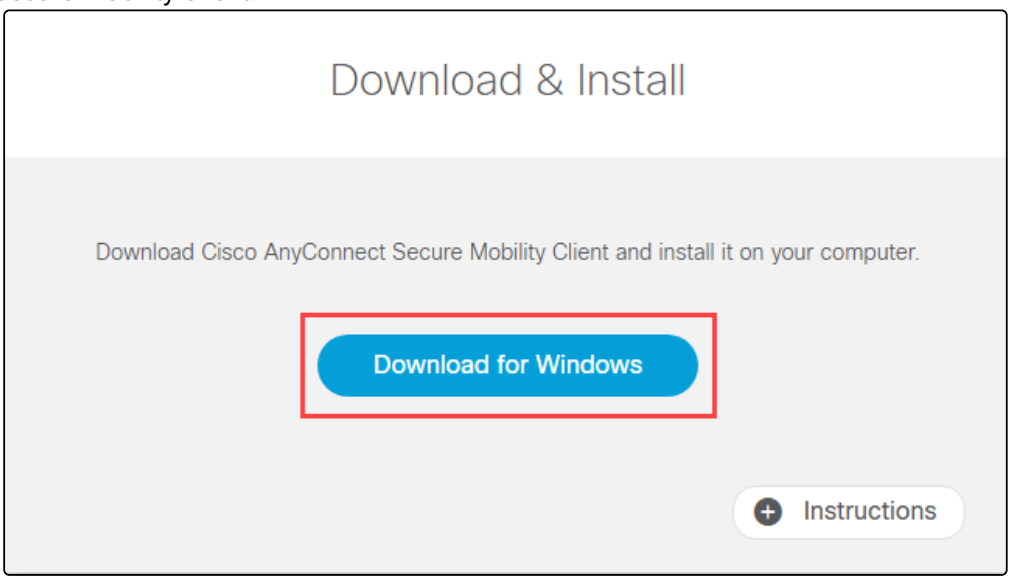
3.4.1.1 Первоначальная установка VPN-клиента

Если VPN-клиент Cisco AnyConnect уже установлен на вашем компьютере, пропустите этот раздел и перейдите к разделу Авторизация по VPN.

1. Откройте в браузере страницу https://vpn.clearwayintegration.com
   Введите логин (без указания домена) и пароль учетной записи VPN-клиента.



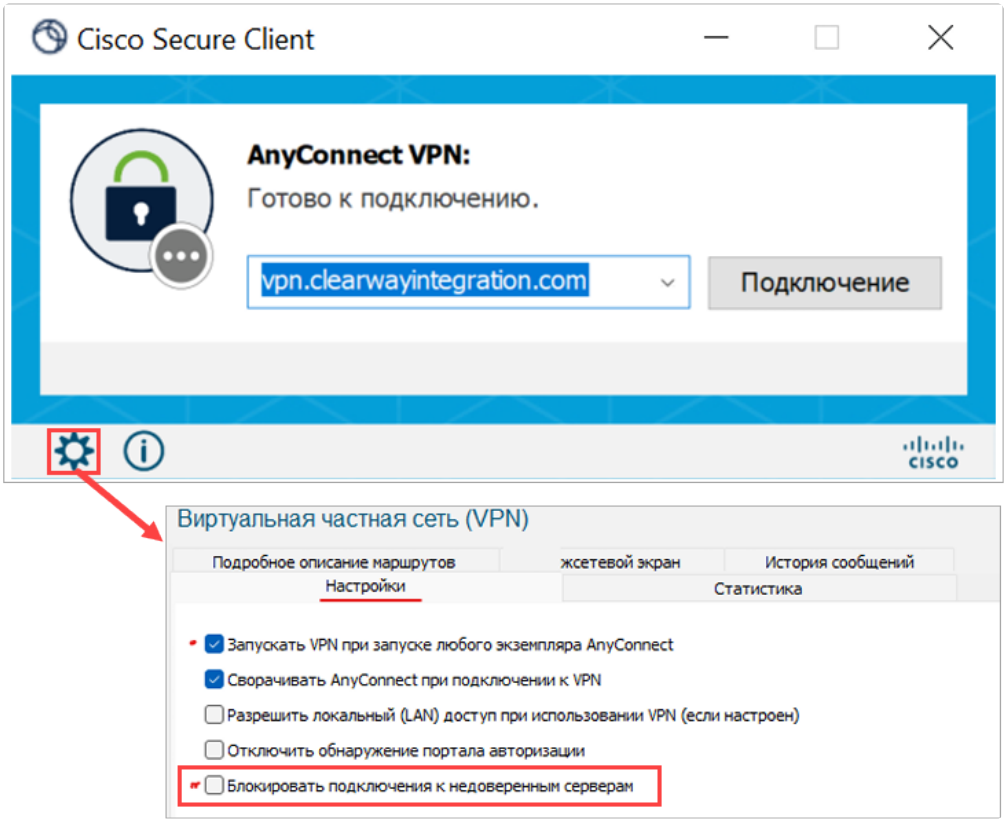
2. После успешной авторизации откроется окно с кнопкой для скачивания дистрибутива AnyConnect Secure Mobility Client.



   Клиент выбирается автоматически для той ОС, в которой открыт браузер.

3. Скачайте и установите Cisco AnyConnect, следуя указаниям мастера установки.
4. Запустите клиент Cisco AnyConnect.

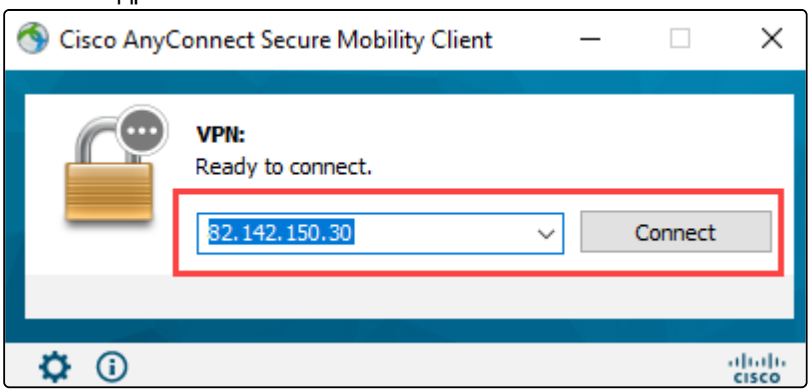
5. Откройте настройки (значок шестеренки) и снимите флажок "Блокировать подключения к недоверенным серверам", затем закройте окно настроек.



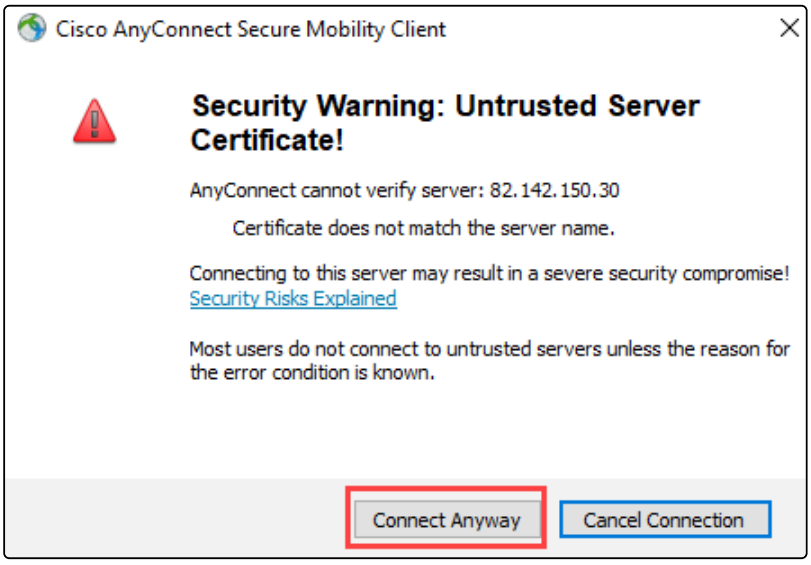
3.4.1.2 Авторизация по VPN

Для подключения к VPN выполните следующие действия.

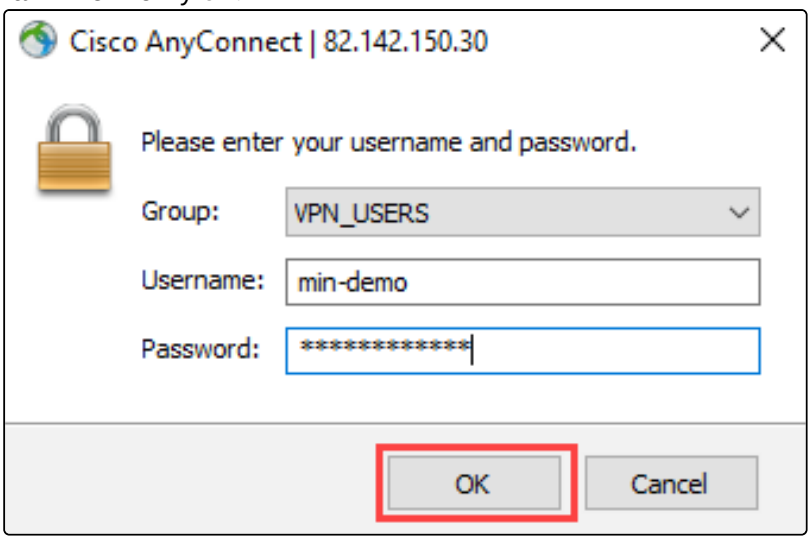
1. Запустите VPN-клиент Cisco AnyConnect.
2. Укажите адрес шлюза и нажмите **Connect**.



3. При подключении к демо-стенду вы можете увидеть предупреждение, что сертификат внутреннего корпоративного ресурса не является доверенным для вашего компьютера. Это не означает, что соединение небезопасно. Нажмите **Connect Anyway**.

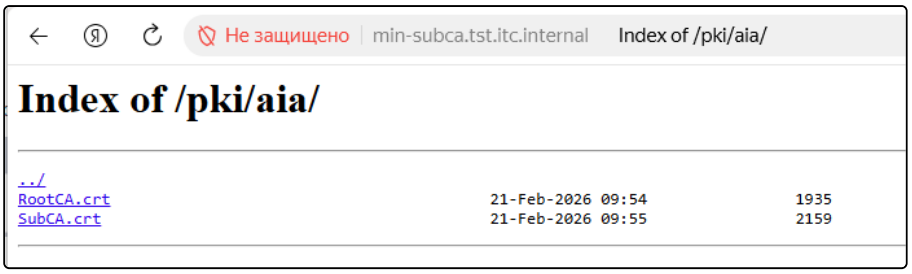


4. Укажите логин и пароль учетной записи VPN-клиента, в поле "Группа" выберите "VPN_USERS".
5. Нажмите кнопку **OK**.



3.4.2 Добавление сертификатов в доверенные

1. Откройте браузер и перейдите по ссылке http://min-subca.tst.itc.internal/pki/aia/.



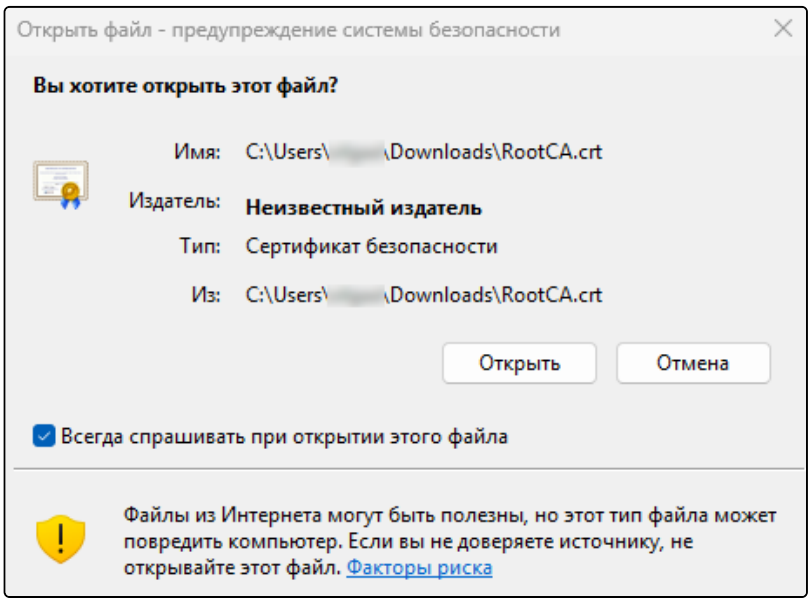
2. Скачайте на компьютер файлы сертификатов *RootCA.crt* и *SubCA.crt*.
3. Перейдите в директорию, куда вы сохранили файлы сертификатов.

4. Добавьте сертификаты, как описано ниже.
5. После добавления сертификатов закройте и заново откройте браузер, чтобы он подхватил новые сертификаты.

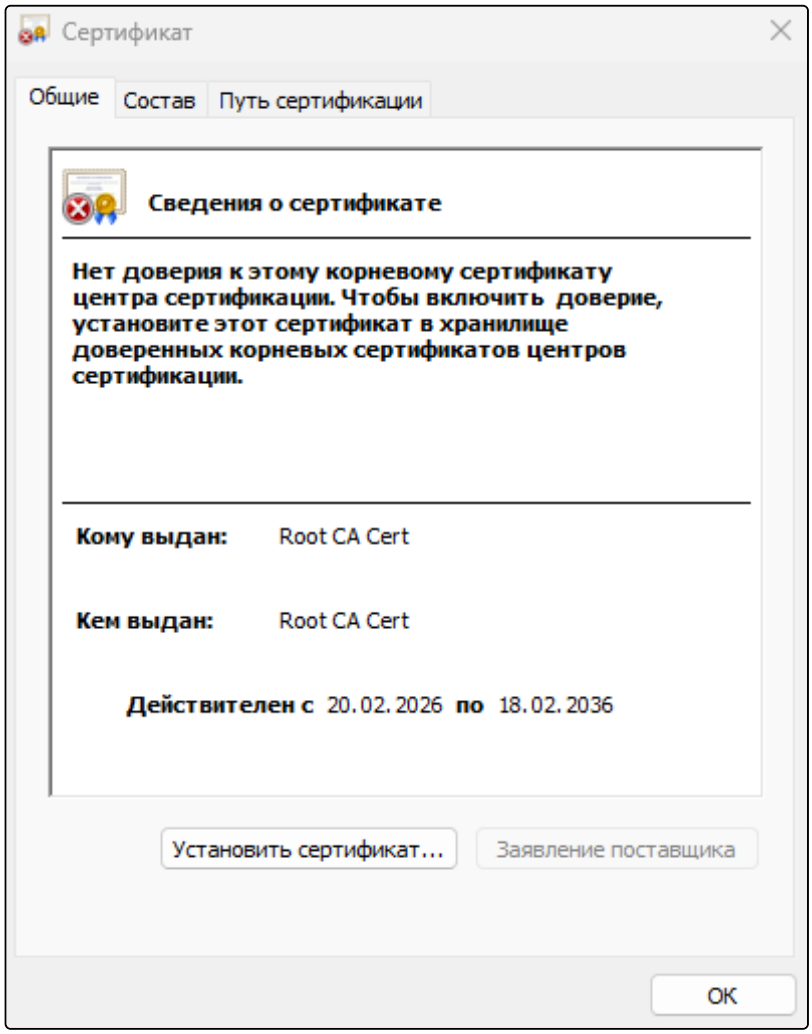
3.4.2.1 Добавление сертификатов для ОС Windows

1. Добавьте корневой сертификат *RootCA.crt* в доверенные корневые центры сертификации.

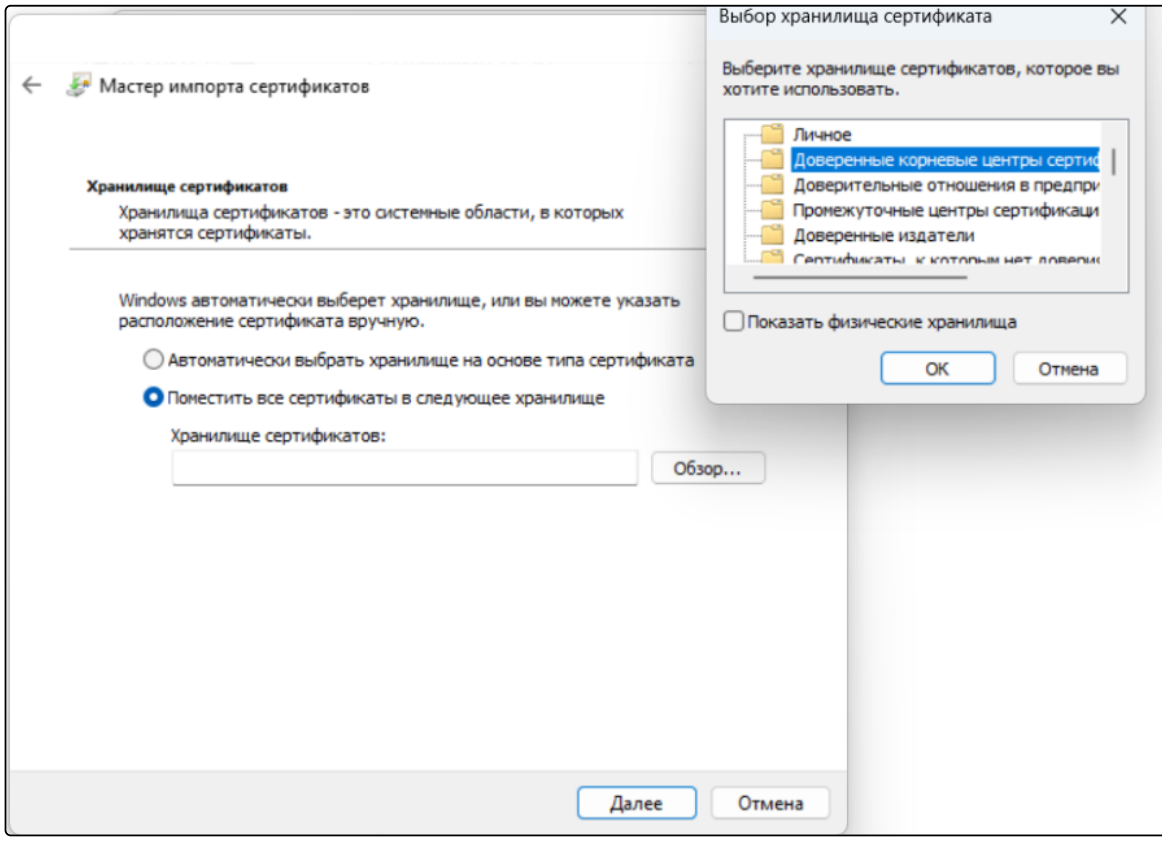
    a. Дважды нажмите на имя файла *RootCA.crt*, а затем в окне предупреждения системы безопасности нажмите **Открыть**.



    b. Нажмите **Установить сертификат**.



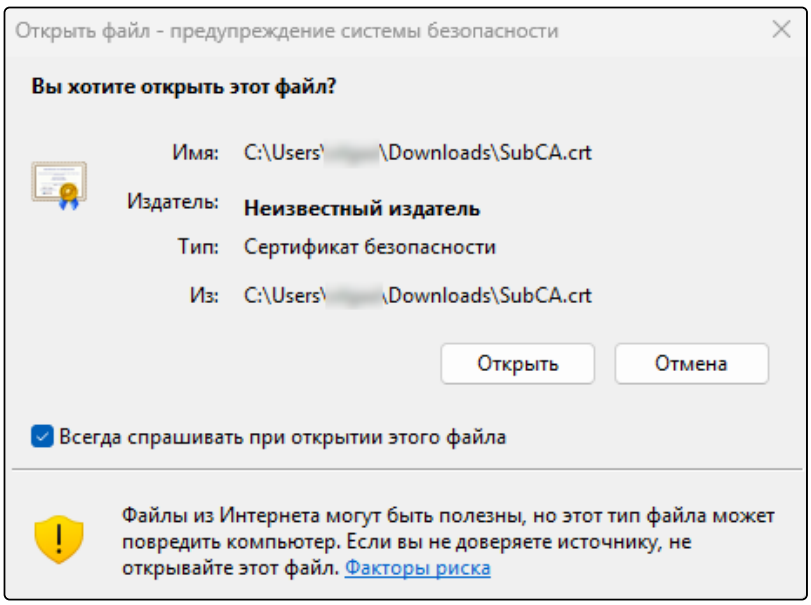
c. Нажмите **Далее**, выберите пункты, как показано на рисунке ниже. Затем нажмите **Далее**.



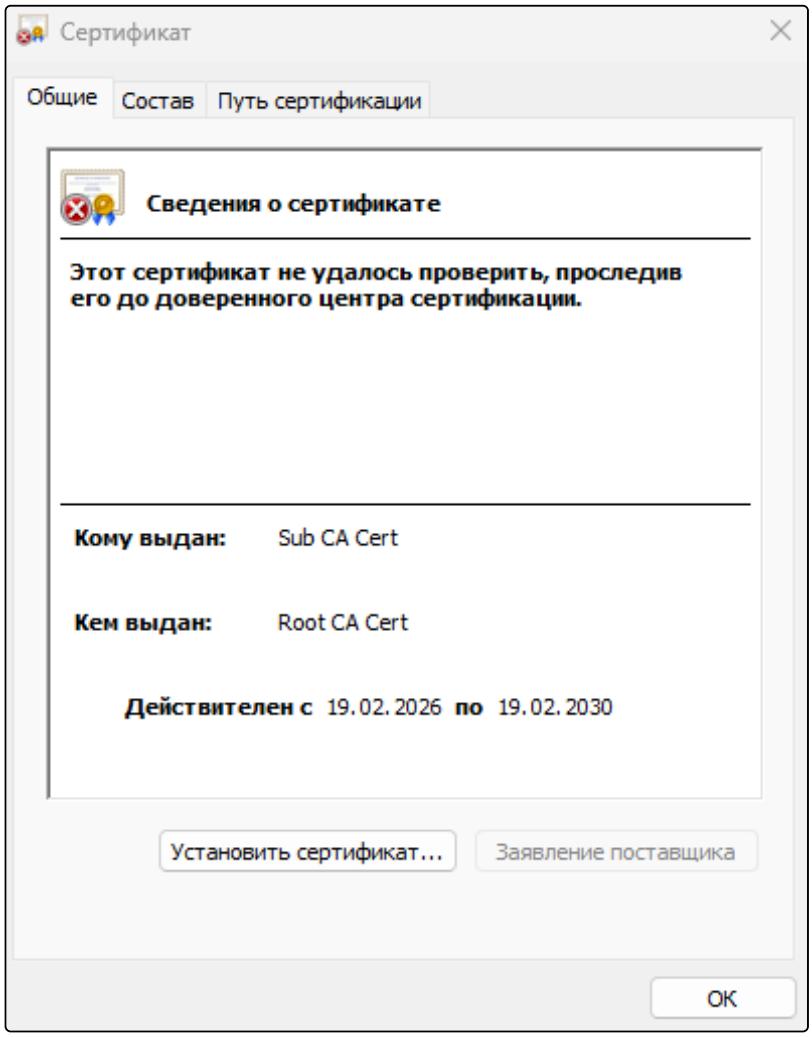
d. Нажмите **Готово**, а затем в окне предупреждения системы безопасности нажмите **Да**.

2. Добавьте промежуточный сертификат *SubCA.crt* в промежуточные центры сертификации:

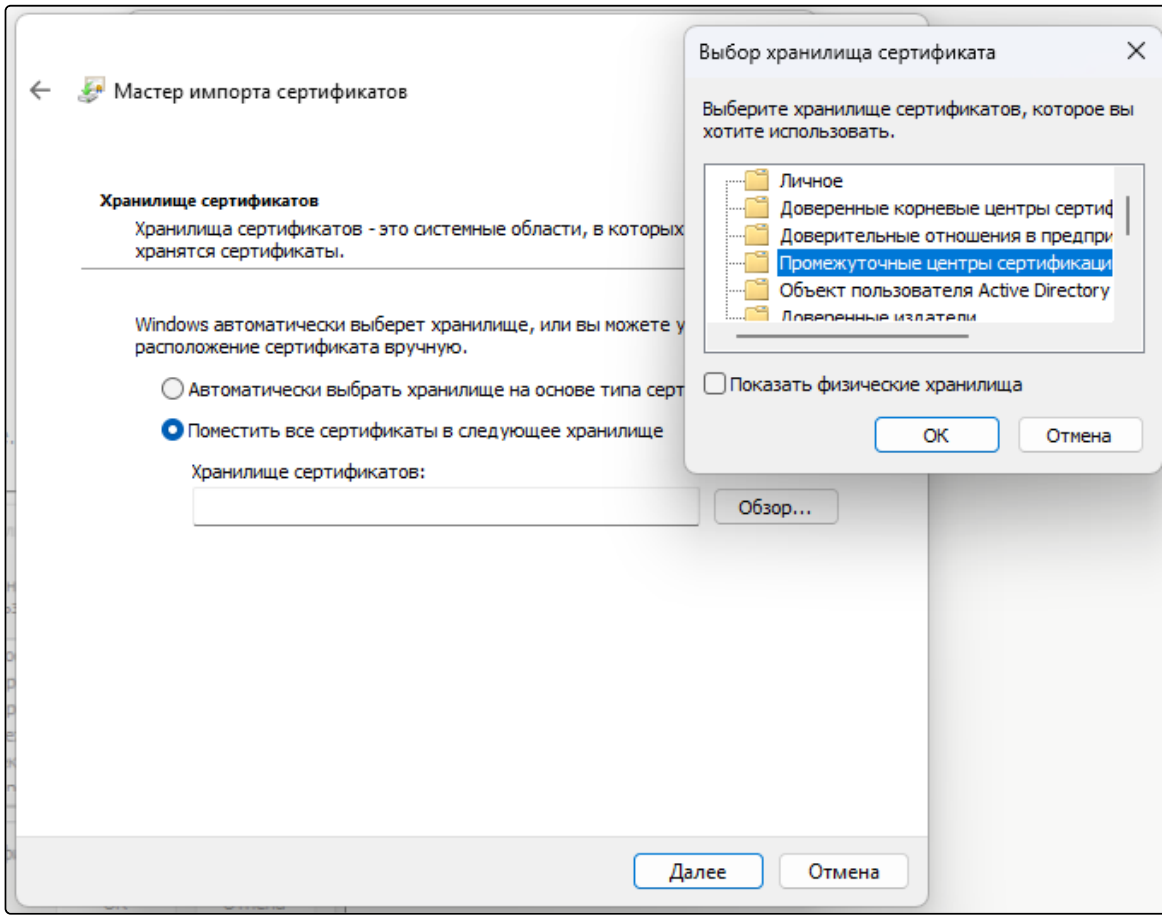
a. Дважды нажмите на имя файла *SubCA.crt*, а затем в окне предупреждения системы безопасности нажмите **Открыть**.



b. Нажмите **Установить сертификат**.



c. Нажмите **Далее**, выберите пункты, как показано на рисунке ниже. Затем нажмите **Далее**.



d. Нажмите **Готово**, а затем в окне предупреждения системы безопасности нажмите **Да**.

3.4.2.2 Добавление сертификата для ОС Linux

3.4.2.2.1 Метод 1. Использование update-ca-certificates (Debian/Ubuntu)

1. Скопируйте сертификат в нужную директорию:

```
sudo cp your-ca-certificate.crt /usr/local/share/ca-certificates/
```

2. Обновите хранилище сертификатов:

```
sudo update-ca-certificates
```

3. Проверьте добавление сертификата:

```
ls -la /etc/ssl/certs/ | grep your-certificate
```

3.4.2.2.2 Метод 2. Ручное добавление (RHEL/CentOS/Fedora)

1. Скопируйте сертификат:

```
sudo cp your-ca-certificate.crt /etc/pki/ca-trust/source/anchors/
```

2. Обновите хранилище сертификатов:

```
sudo update-ca-trust
```

3. Проверьте добавление сертификата:

```
ls -la /etc/pki/ca-trust/extracted/openssl/
```

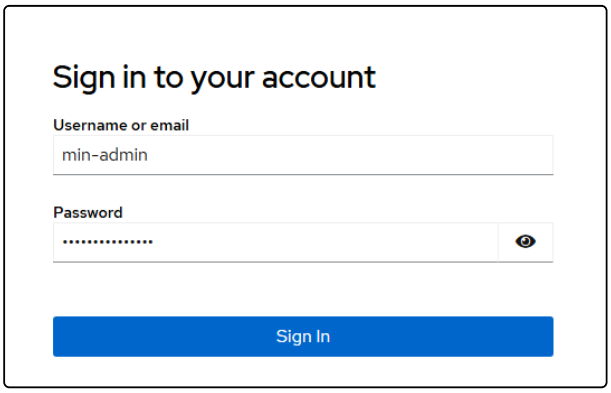
3.5 Вход в веб-интерфейс демо-стенда

Для начала работы с веб-интерфейсом системы выполните следующие шаги:

Предварительные требования
Убедитесь, что ваше рабочее место подключено к корпоративной сети через VPN (см. раздел Настройка доступа), так как адрес находится во внутреннем контуре.

Порядок действий

1. Откройте используемый веб-браузер (например, Google Chrome, MS Edge или Яндекс.Браузер).
2. В адресную строку введите следующую ссылку и нажмите **Enter**: https://min-smiok.tst.itc.internal/.
3. В появившемся окне входа заполните соответствующие поля, используя данные из таблицы Учетные записи.



4. После ввода данных нажмите кнопку входа для доступа к главной странице системы. Откроется главная страница портала СМИОК.

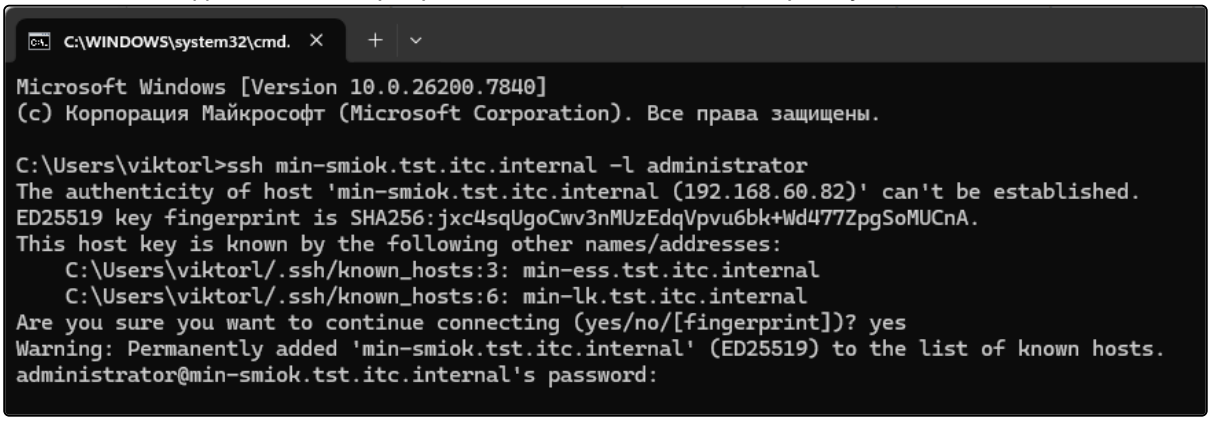
Рисунок 1 Главная страница портала СМИОК

3.6 Подключение к демо-стенду через SSH

> Для подключения к демо-стенду через SSH запросите учетные данные администратора у сотрудников технической поддержки.

Для подключения можно использовать стандартный SSH-клиент (OpenSSH), который вызывается через командную строку (cmd) для Windows, или использовать стандартный терминал для Linux.

1. Введите команду для подключение к машине демо-стенда по SSH: `ssh min-smiok.tst.itc.internal -l administrator`
2. Согласитесь на добавление сервера в known_hosts, вписав в строке yes.



3. Введите пароль от учетной записи `administrator`.

4. При успешном подключении вы увидите информацию о предыдущем входе пользователя, а в начале строки появится имя пользователя и имя сервера.

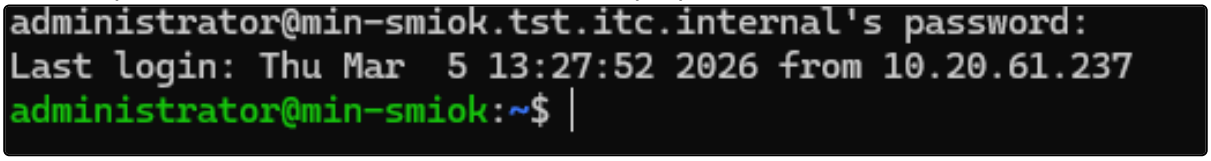


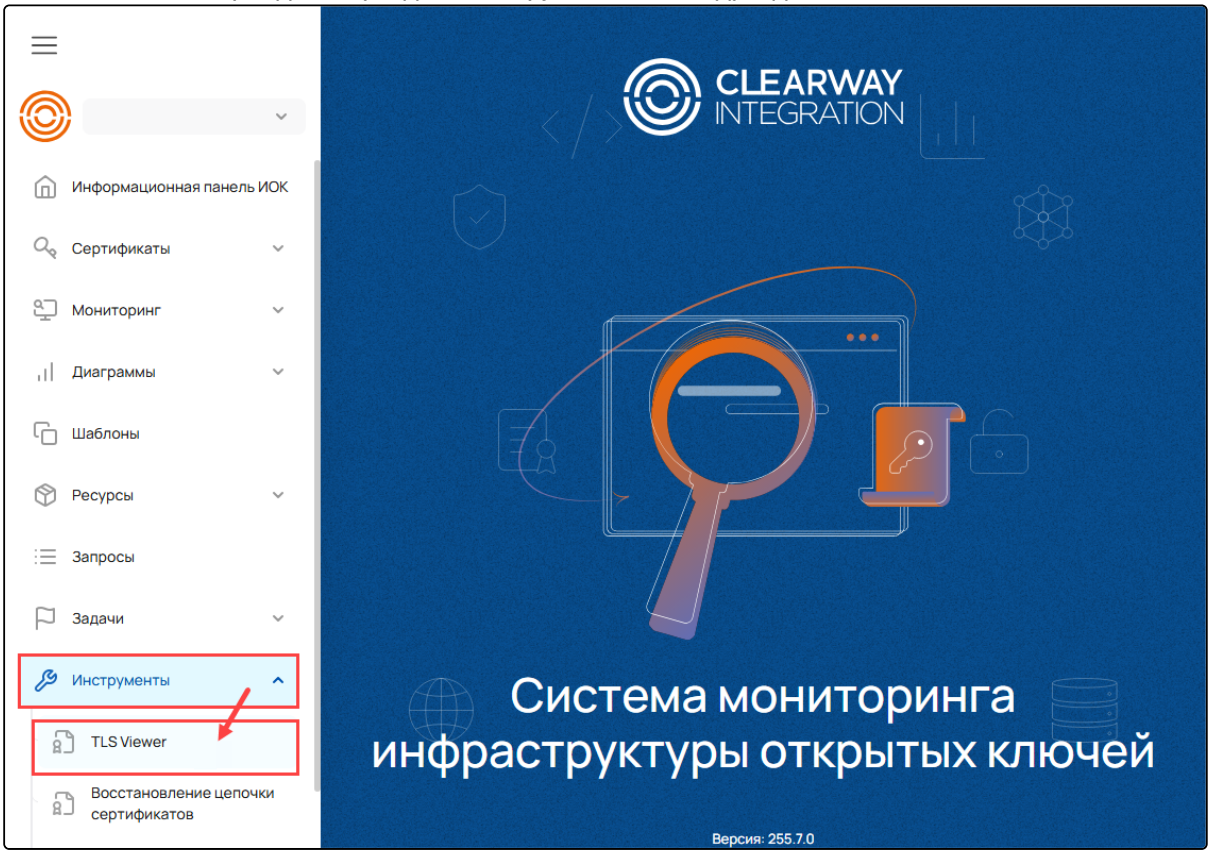
Рисунок 2 Успешное подключение по ssh

4 Проверка работы ПО

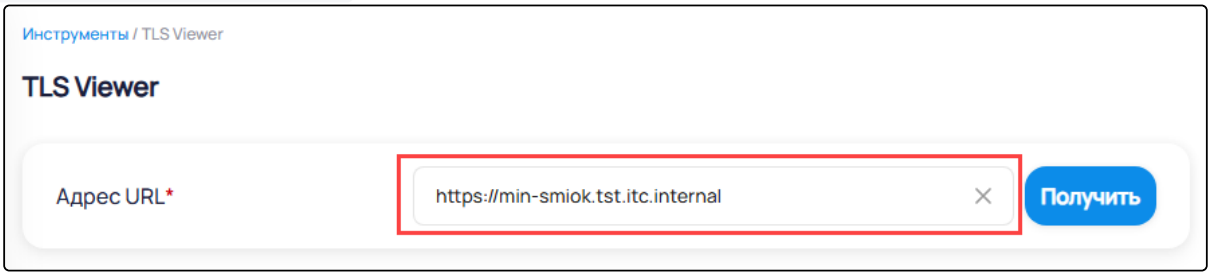
4.1 Просмотр и скачивание сертификата (TLS Viewer)

Проверяется возможность получения цепочки TLS-сертификатов сервера по HTTPS-адресу и скачивания любого сертификата из цепочки в формате DER или PEM.

1. Перейдите в веб-интерфейс управления системой (см. раздел Вход в веб-интерфейс системы).
2. Откройте подраздел «TLS Viewer»
   В главном меню перейдите в раздел «Инструменты» → подраздел «TLS Viewer».



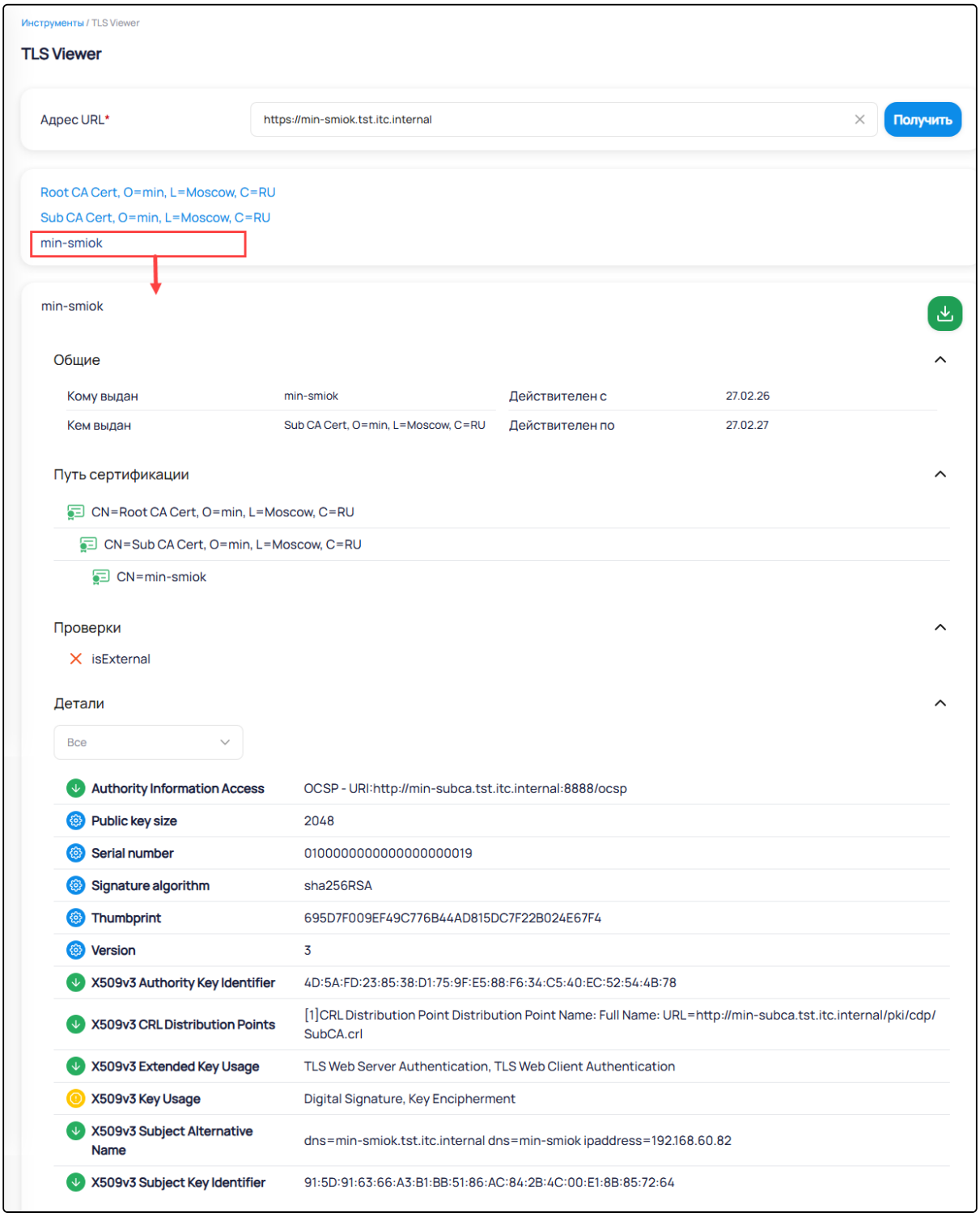
3. Укажите HTTPS-адрес сервера
   В поле «Адрес URL» введите полный адрес сервера, например, `https://min-smiok.tst.itc.internal`.



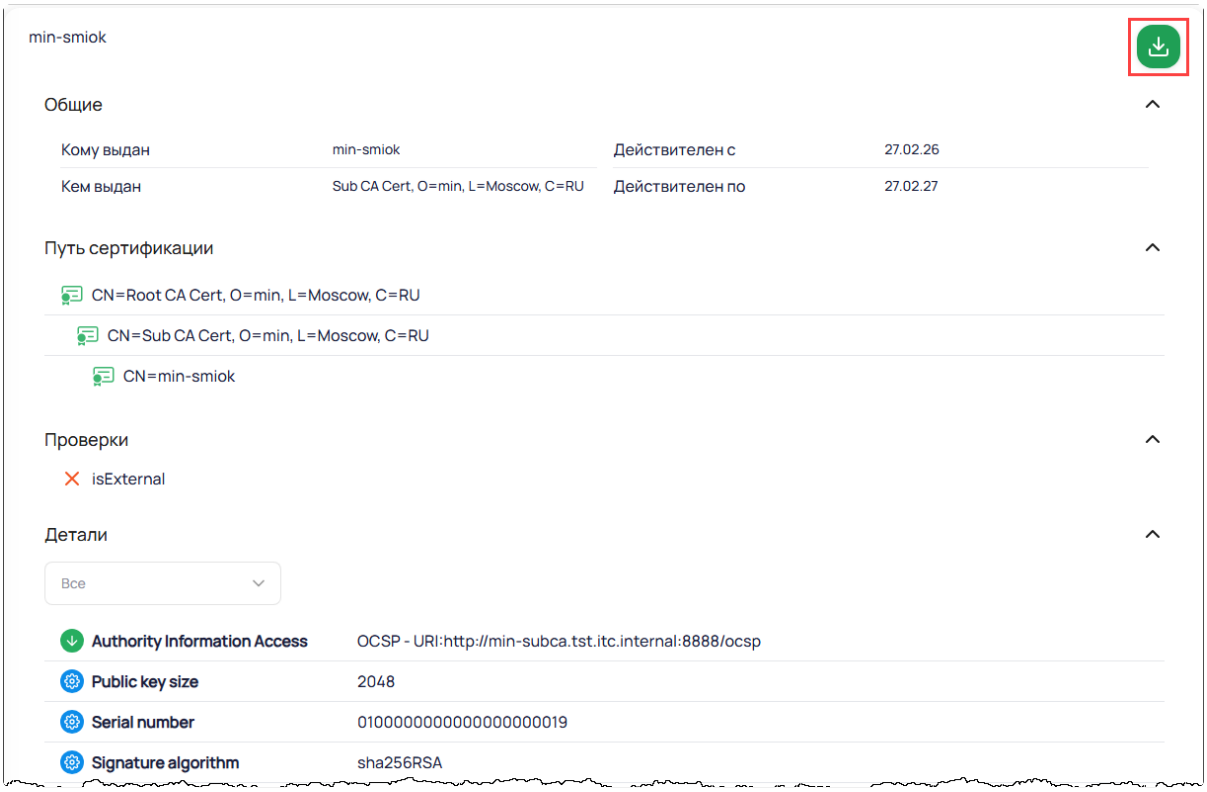
4. Получите сертификаты сервера
   Нажмите кнопку **Получить**.

   Система устанавливает защищенное соединение и получает сертификаты сервера.

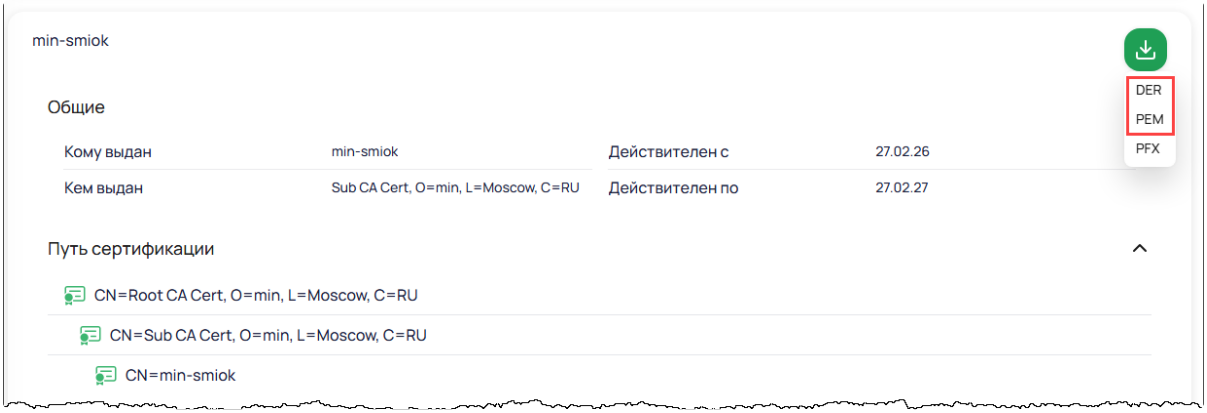
5. Перейдите к просмотру сертификата
   В отобразившейся иерархии сертификатов кликните левой кнопкой мыши на любом сертификате и ознакомьтесь с информацией в открывшейся карточке сертификата.



6. Приступите к сохранению сертификата на локальном диске
   В правом верхнем углу карточки сертификата нажмите кнопку зеленого цвета с обозначением действия скачивания  .



7. Выберите формат сертификата
   Из раскрывающегося списка выберите требуемый формат скачиваемого сертификата (DER или PEM).

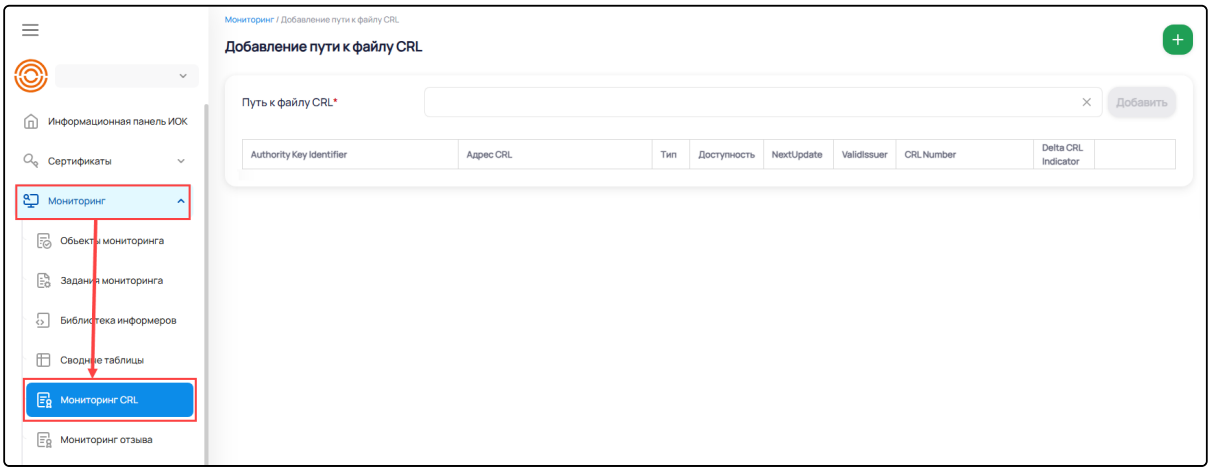


8. Сертификат успешно сохраняется на локальном диске
   Файл скачивается в директорию, заданную на вашем компьютере для сохранения загруженных документов.

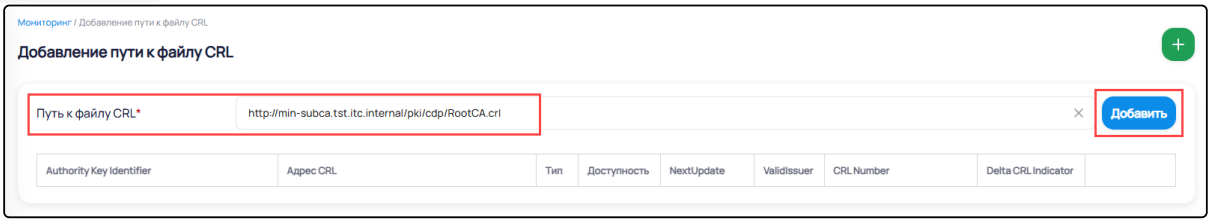
4.2 Отслеживание отозванных сертификатов (CRL)

Проверяется добавление CRL-файла на мониторинг и отображение его в списке объектов мониторинга.

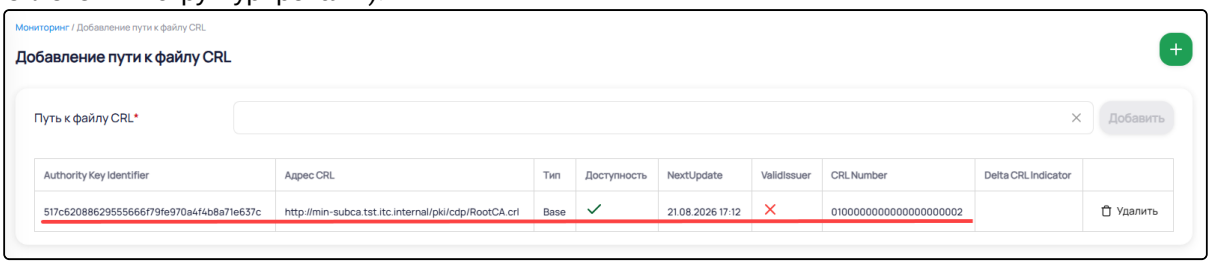
1. Перейдите в веб-интерфейс управления системой (см. раздел Вход в веб-интерфейс системы).
2. Откройте подраздел «Мониторинг CRL»
   В главном меню перейдите в раздел «Мониторинг» → подраздел «Мониторинг CRL».



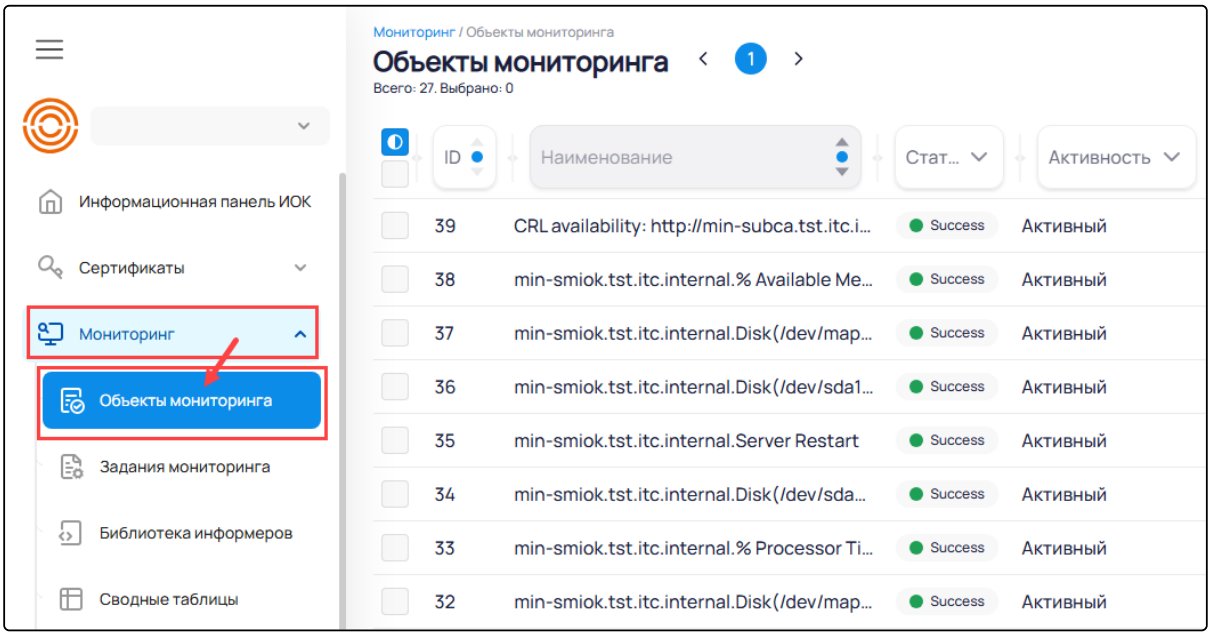
3. Добавьте сертификат
   Укажите путь к CRL-файлу, например, `http://min-subca.tst.itc.internal/pki/cdp/RootCA.crl` и нажмите кнопку **Добавить**.



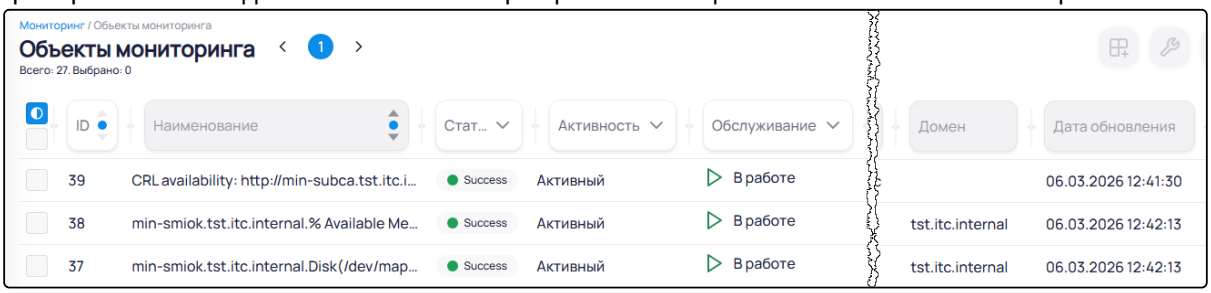
4. Новая строка в таблицу CRL-сертификатов добавлена
   Убедитесь, что в таблице появилась новая строка с добавленным CRL (данные должны быть извлечены и структурированы).



5. Откройте подраздел «Объекты мониторинга»
   Подождите 10 минут (время обработки данных).
   Перейдите в раздел «Мониторинг» → подраздел «Объекты мониторинга».



6. Добавленный сертификат отображается в списке объектов мониторинга
   Проверьте наличие добавленного CRL-сертификата в общем списке объектов мониторинга.



4.3 Добавление внешнего сертификата

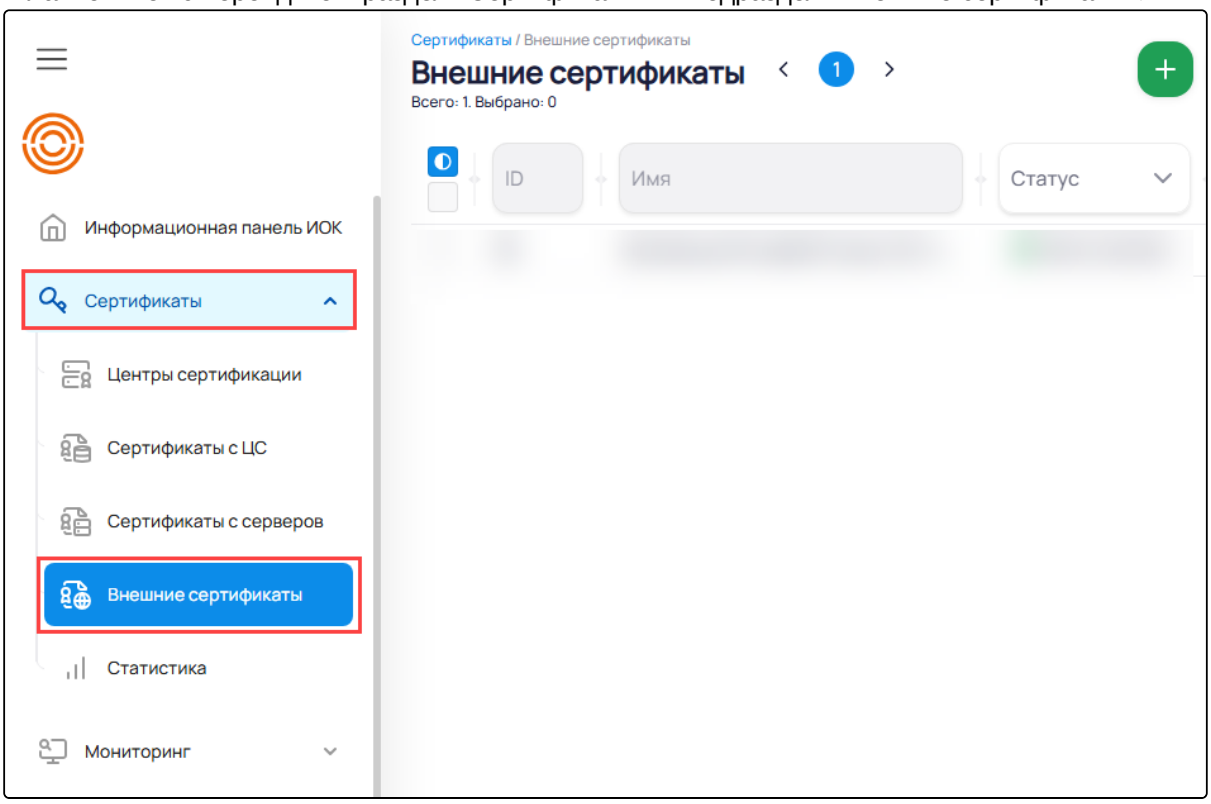
Проверка добавления внешнего сертификата в систему и его отображения в списке внешних сертификатов.

Для выполнения данной проверки, потребуется сертификат. Можете использовать свой сертификат или воспользоваться данным сертификатом для теста:

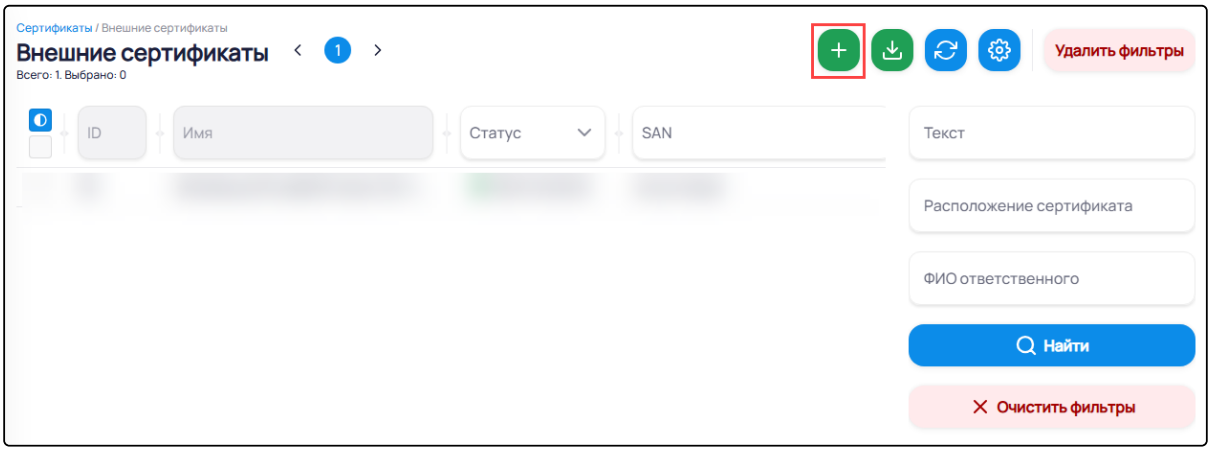
```
-----BEGIN CERTIFICATE-----
MIIEtTCCA52gAwIBAgILEAAAAAAAAAAAAYMwDQYJKoZIhvcNAQELBQAwgZYxCzAJ
BgNVBAYTAlJVMQ8wDQYDVQQIDAZNb3Njb3cxHTAbBgNVBAoMFENsZWFyd2F5IElu
dGVncmF0aW9uMRowGAYDVQQLDBFJVEMtTUNBMS1JbnRlcm5hbDEaMBgGA1UEAwwR
SVRDLU1DQTEtSW50ZXJuYWwxHzAdBgkqhkiG9w0BCQEWEHNzbEBpdGMuaW50ZXJu
YWwwHhcNMjYwMTEwMTAyMjI4WhcNMjcwMTEwMTEyMjI4WjAsMSowKAYDVQQDEyFr
bm93bGVkZ2UuY2xlYXJ3YXlpbnRlZ3JhdGlvbi5jb20wggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQDfcxEfZD23RFUFFhNL1O06T7foxhLNmdJrU2JjAwfh
N+ph3OtLZA2EIkFvfjBX++Ak3rt/Kkky+ZPKBTIWM34tji8aqhOsB8IAYTWZ4CFJ
KFQA6NmWaiWQN6KqSEXLoVkNaF6T93d5O1ayxJIstHiuaa4F5LBl2X4fw2P/MQqk
xac6O72z/Sv/s5JxhnAwG7dKvrF7NPxEezNF1b4IevyLU2IlYbWWymrb9Z/fxQGI
QYzOck5rAIe/MrT1fV89lNoaQjDFq/TZMx8AxkgHQTOVUrdJOv0Ftg9B3AInfkMC
```

```
OOPPdpgUPfte7zAeXr19JC/85cBfbQdJDB5P4wUqokGvAgMBAAGjggFrMIIBZzAO
BgNVHQ8BAf8EBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMB0G
A1UdDgQWBBRcxv9054cNWDjGcdV5n8ElqYrzezAfBgNVHSMEGDAWgBSrsDgaitBG
yf2icV1+kUtA0MWK4zBOBgNVHR8ERzBFMEOgQaA/hj1odHRwOi8vaXRjLWVzYXUt
YjEuaXRjLmludGVybmFsL3BraS9jZHAvaXRjLWludGVybmFsLW1jYTEuY3JsMFkG
CCsGAQUFBwEBBE0wSzBJBggrBgEFBQcwAoY9aHR0cDovL2l0Yy1lc2F1LWIxLml0
Yy5pbnRlcm5hbC9wa2kvYWlhL2l0Yy1pbnRlcm5hbC1tY2ExLmNydDBLBgNVHREE
RDBCgiFrbm93bGVkZ2UuY2xlYXJ3YXlpbnRlZ3JhdGlvbi5jb22CHWtub3dsZWRn
ZS5sYWIuaXRjLmludGVybmFsZGV2MA0GCSqGSIb3DQEBCwUAA4IBAQCdEWsq/YqD
2twhgDdbzpC5kU5gj/Rxuuw02ysZJXZ4Vme25jkPv7QwG39v5vv3RnLCZCOgk7rE
OHDXp/+kHZ2RKcG6+suyMfxwrjHt1CCv8+3kTDl0E9V9cj/g2aA64SgRCYHhnlMj
PY5B64xGK/yFjGrr1Z9LB3Q155vabqOSqFQ3ewURwSKSIoYQTNNhrt8+9/RFSFRI
GFlkJvyLXv+cgxf4xEHBZfTXXnoGYzpObJxhyqfdg8ntKrpFGcSjK5gOmJq51Kav
OW1qdtnGigu3MzsRxYYj1AElZhLO4HDBfXJfufQipcU10s0SF/Ht6Lk2B9xrJTRV
SaJ9umdlQVXu
-----END CERTIFICATE-----
```

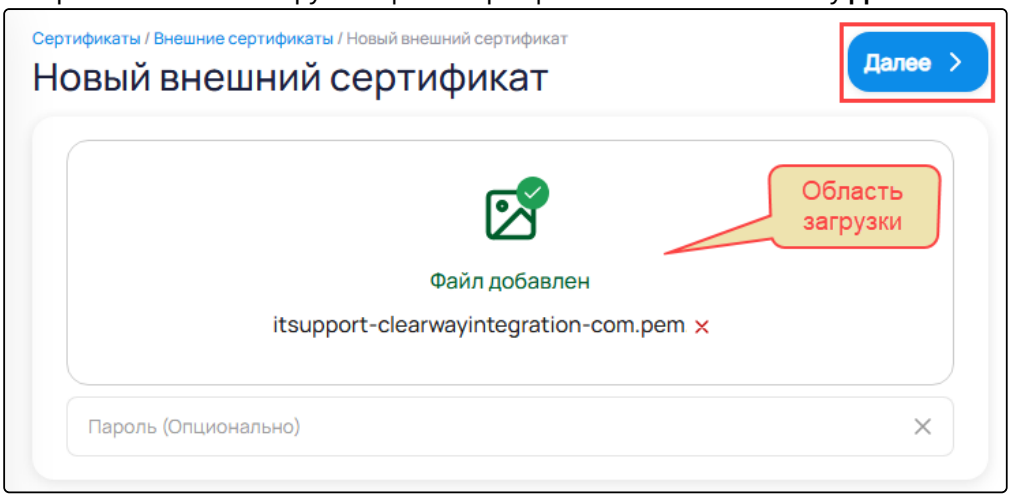
1. Перейдите в веб-интерфейс управления системой (см. раздел Вход в веб-интерфейс системы).
2. Откройте подраздел «Внешние сертификаты»
   В главном меню перейдите в раздел «Сертификаты» → подраздел «Внешние сертификаты».



3. Приступите к добавлению сертификата
   Нажмите кнопку «+» в правом верхнем углу.



4. Загрузите файл сертификата
   В открывшемся окне загрузите файл сертификата и нажмите кнопку **Далее**.



5. Заполните все обязательные поля в карточке сертификата
   Обязательные поля формы:
   - Ответственный сотрудник (ФИО);
   - E-mail ответственного;
   - Общий комментарий;
   - Место установки;
   - Количество дней до конца срока действия сертификата.

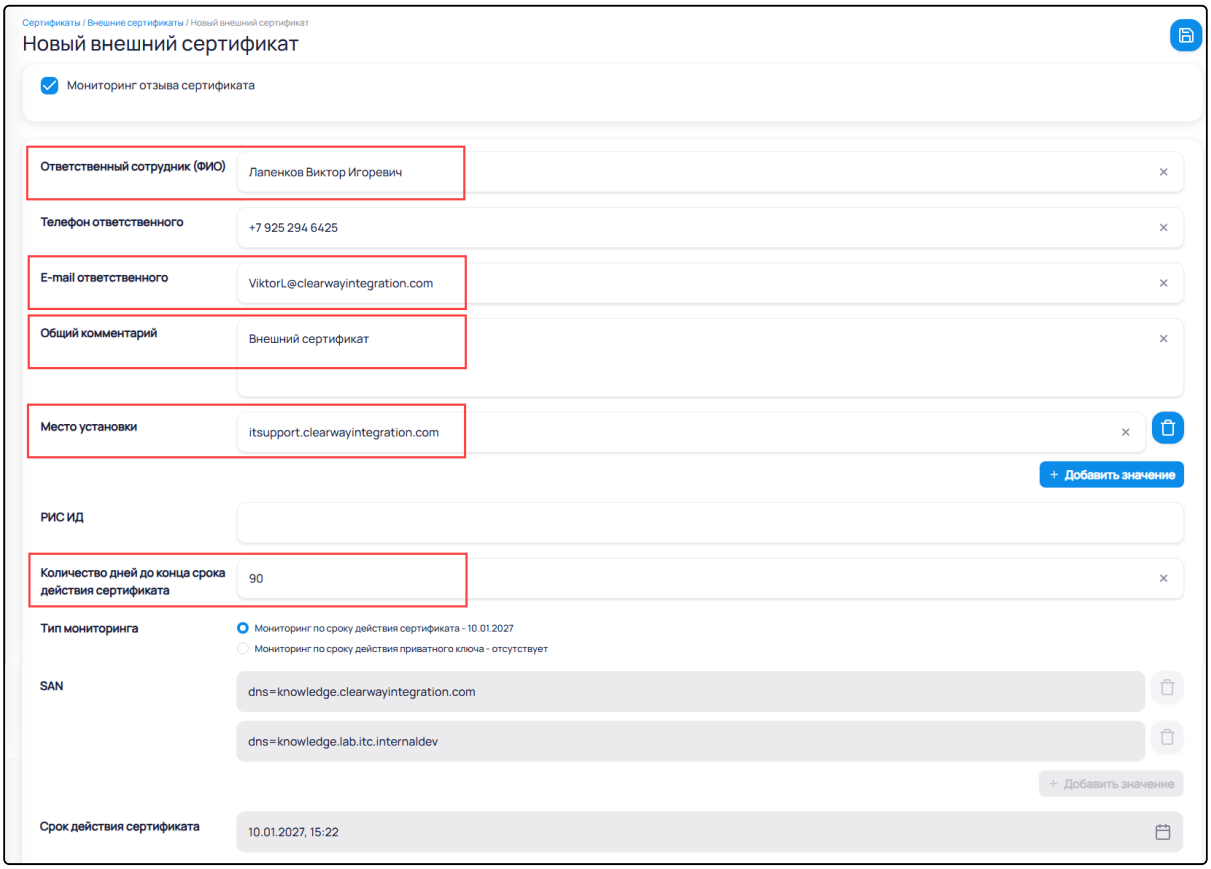
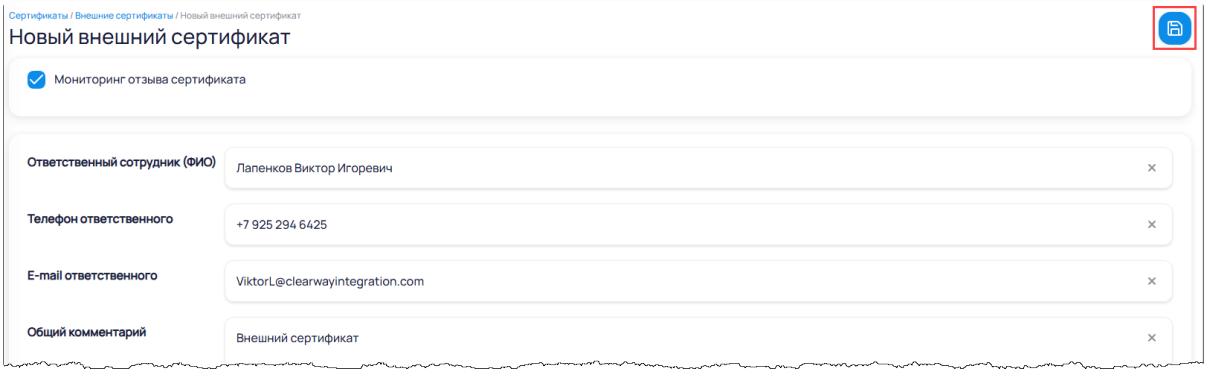


Рисунок 3 Заполнение карточки внешнего сертификата

6. Сохраните внешний сертификат в системе

   Нажмите кнопку (Сохранить) в правом верхнем углу.



7. Сертификат сохранен

   В правом верхнем углу окна появится уведомление о сохранении сертификата и откроется карточка сохраненного сертификата.

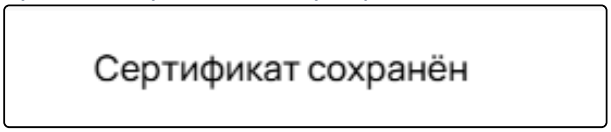


Рисунок 4 Уведомление о сохранении сертификата

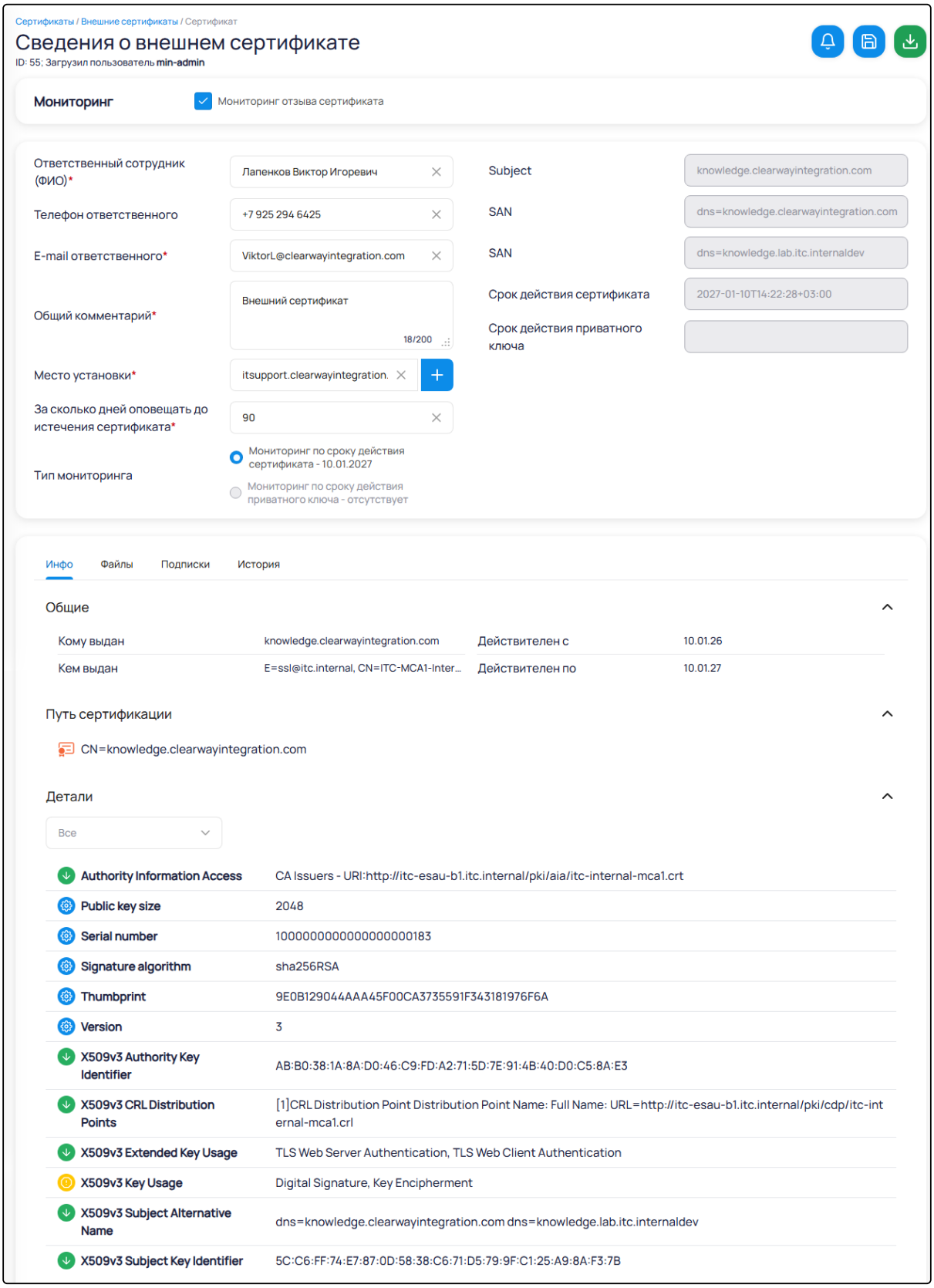


Рисунок 5 Сохраненная карточка внешнего сертификата

8. Добавленный сертификат отображается в списке внешних сертификатов
   Вернитесь в список «Внешние сертификаты» (в главном меню раздел «Сертификаты» →

подраздел «Внешние сертификаты») и обновите страницу браузера (или используйте кнопку обновления).
Проверьте наличие добавленного сертификата в списке.

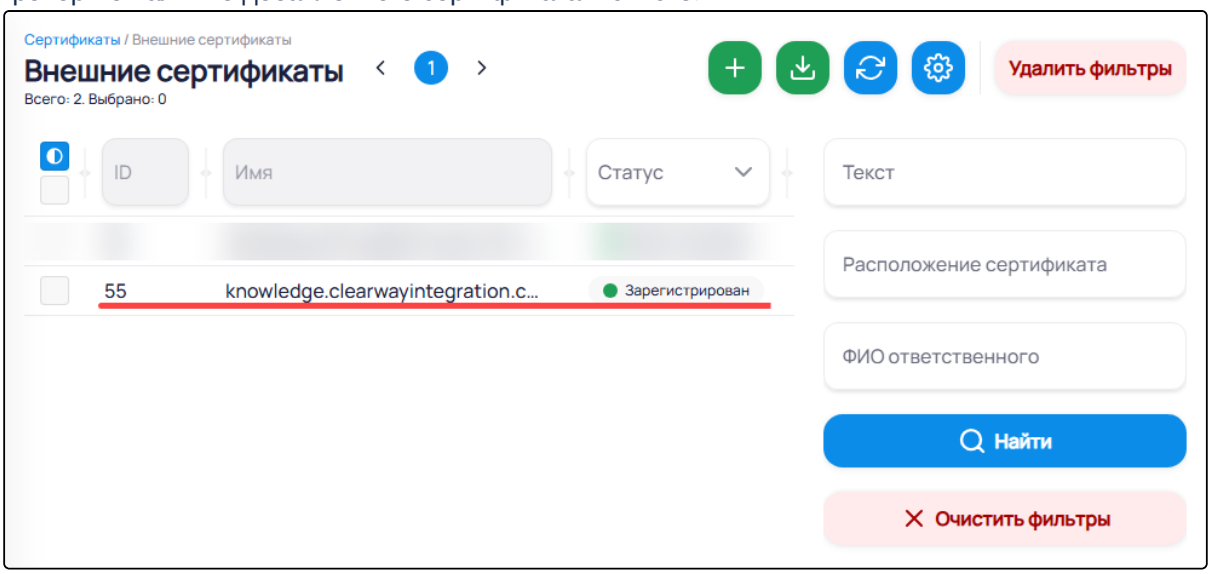
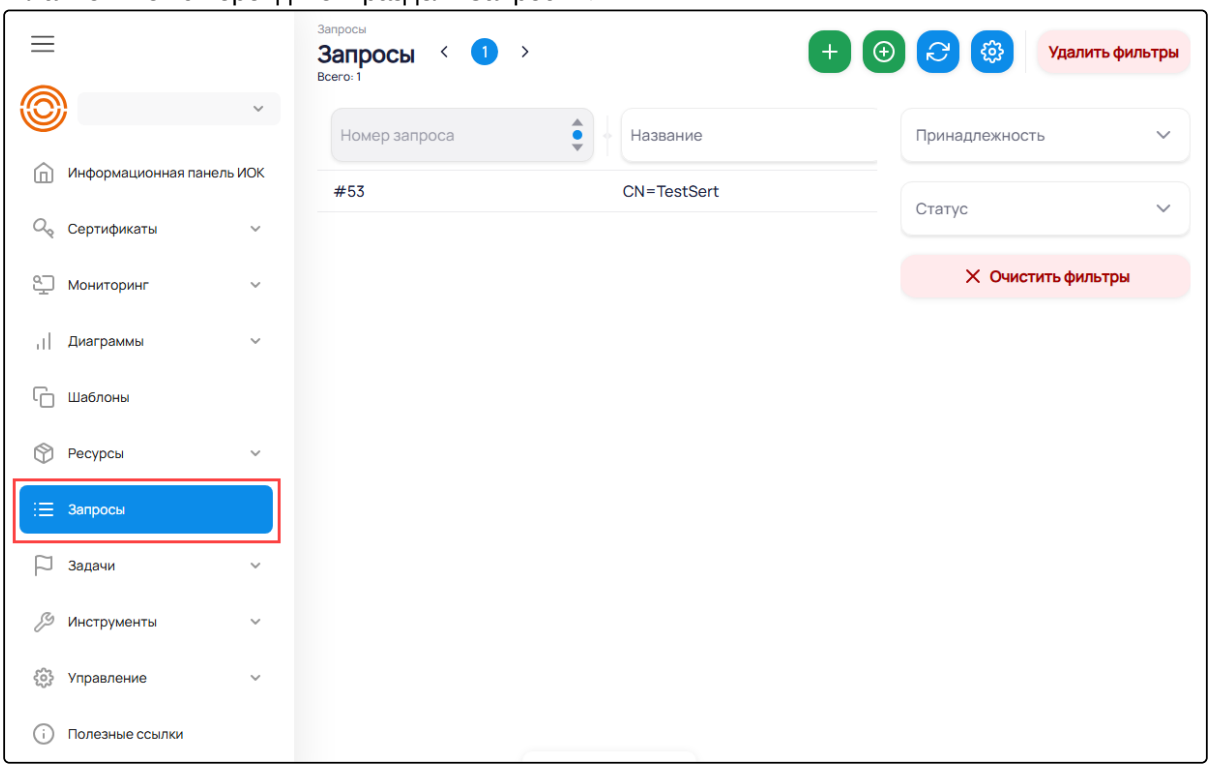


Рисунок 6 Новый внешний сертификат отображается в таблице сертификатов

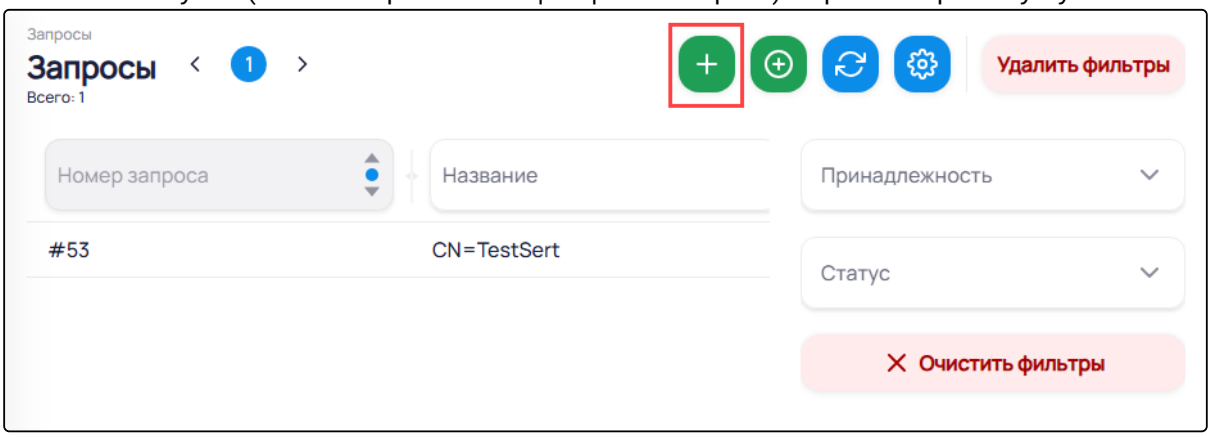
4.4 Выпуск сертификата через файл запроса

Проверка возможности выпуска сертификата через файл запроса с последующим утверждением и отображением в списке сертификатов с ЦС.

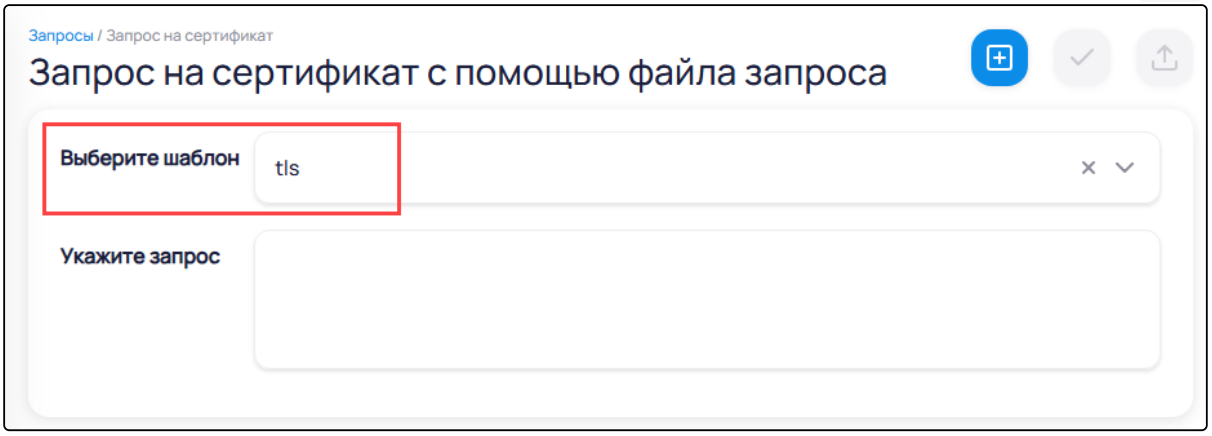
1. Перейдите в веб-интерфейс управления системой (см. раздел Вход в веб-интерфейс системы).
2. Откройте раздел «Запросы»
   В главном меню перейдите в раздел «Запросы».



3. Приступите к созданию нового запроса
   Нажмите кнопку «+» (Новый запрос с помощью файла запроса) в правом верхнем углу.



4. Выберите шаблон
   В открывшемся окне «Запрос на сертификат с помощью файла запроса» выберите шаблон `tls`.



5. Укажите текст запроса
   Введите текст запроса на сертификат (CSR) в поле «Запросы» и нажмите кнопку (Отправить) в правом верхнем углу.
   Пример тестового запроса:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICtzCCAZ8CAQAwFDESMBAGA1UEAwwJc21pb2t0ZXN0MIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEA0iCaQlqAEohOXqPvTRWP6G0Yjraz2IFdX0+ogtZx
S3I2Gg7Z43O1l6kc2R1O+Mb5KjnOQpsB7V9WVnHokOxvBA+ZWnXs0kDCQHPZbkL2
VWetVoaulMHf37YzDQoi5mFUhEzEd5z45oTKli5z2F7JnX78ONtgSzzgOqhgB6+/
uOvu9GbDrxHC0MsCpxBeyAYxP6gFLe0b7drVyzNGKtlKHMP2VUKRVJWZjuBsv9DK
/kOpeLD5ABx83kkuFkE5atL91YObd0/iFQpMOpzkXIa9hp/Czx6khlBheypy5Uqs
l5kXShOPlcwu2VdusDRVA1Yl8yAec7nr6Ew5B46Y+yUuOwIDAQABoF4wXAYJKoZI
hvcNAQkOMU8wTTAsBgNVHREEJTAjghZzbWlva3Rlc3QuYWRkYzAxLmxvY2Fsgglz
bWlva3Rlc3QwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMA0GCSqGSIb3
DQEBCwUAA4IBAQAkzh5I3ZvH3GOLTwu1rFAl5/FZSPPwtyqWmtcH2ZkIZCLN8EcA
MOMDgrn8swhUqFHBNwVjv42D17Di19z6AwF3oGv8p4Zo183mVTZOznNBDKE47LII
```

```
9ACehLTLZq4UjTp0fH/4O74FEYtSgCc1GIGWlZFmdr2vM3zzG3hZzZwYEf+d9sxI
N1rYGoiQoOQwe99rKnTWwzRCPIgXJIQBWkkgLmYXeof1DmTdmbVuGY28ajBFuN8Z
8/oFwQ7dua8q9Hmef0Thj3ntM/J2ITcxiUt4rBSuP+cHCnqS1D8BLkP0eO4wNoa1
udRuhcNKoci+cFVKOZt5UkIfU5kUOlOKCUQm
-----END CERTIFICATE REQUEST-----
```

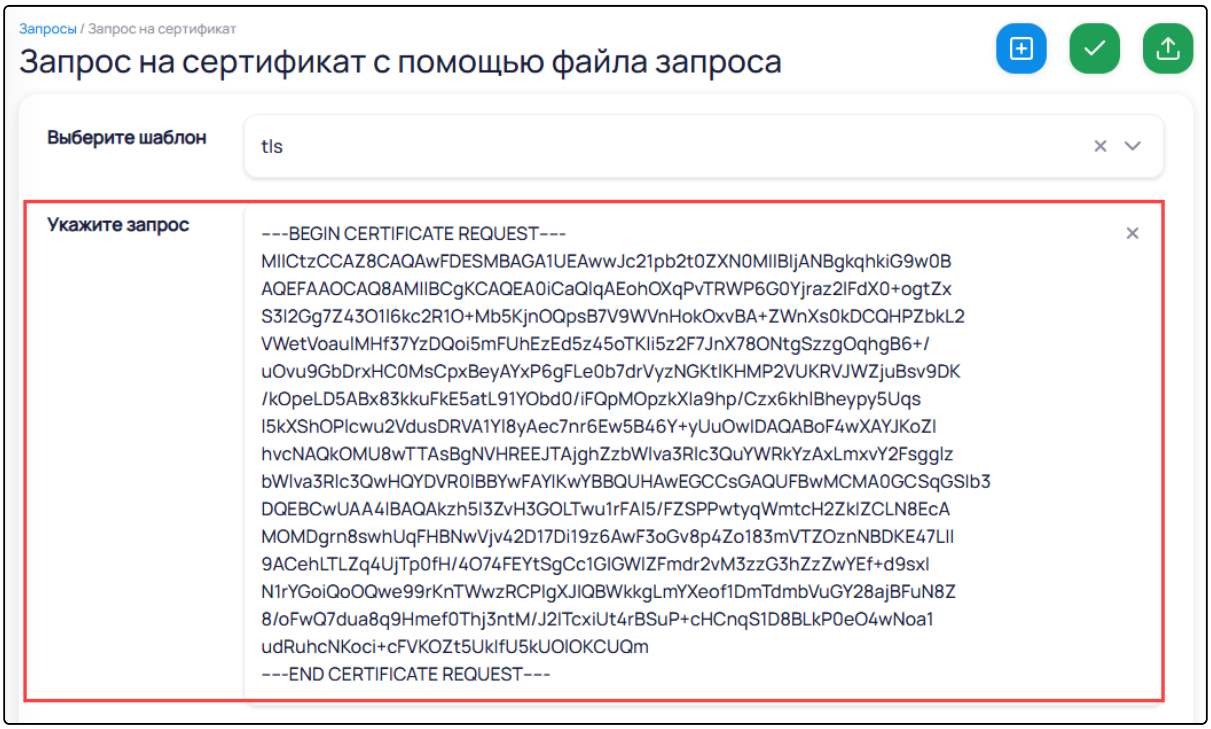
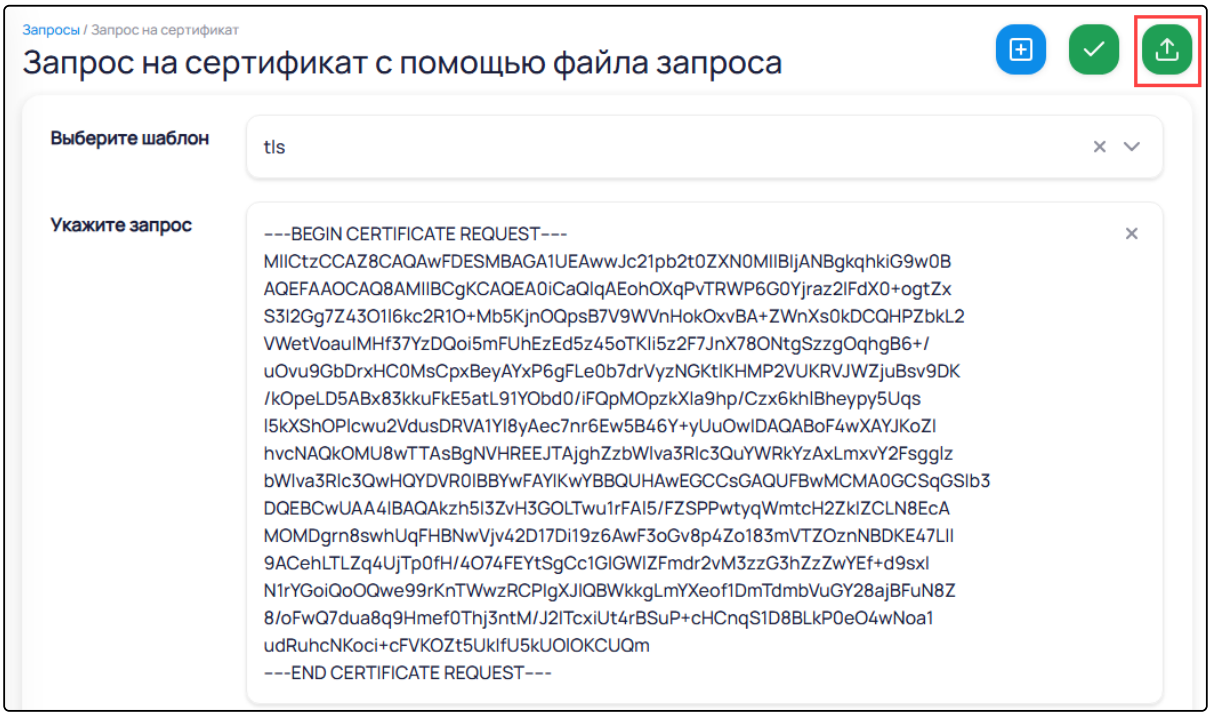


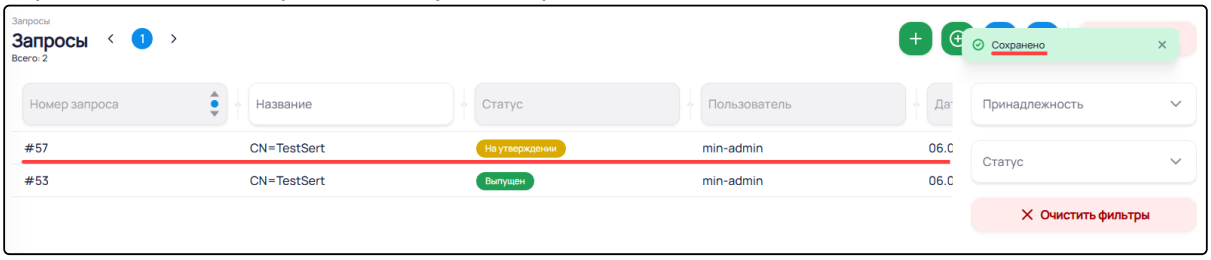
Рисунок 7 Ввод текста запроса

6. Отправьте запрос

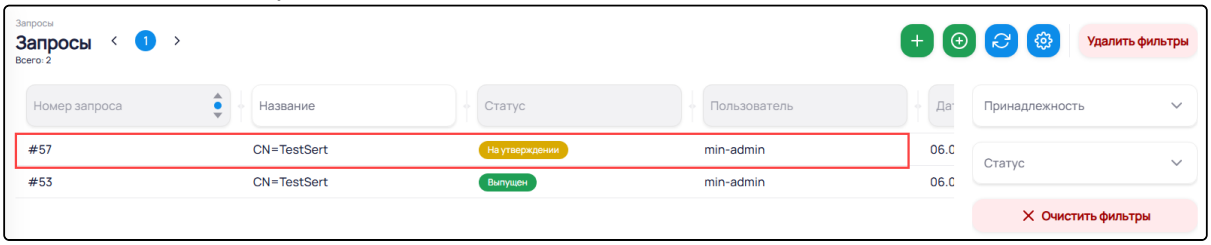
   Нажмите кнопку (Отправить) в правом верхнем углу.



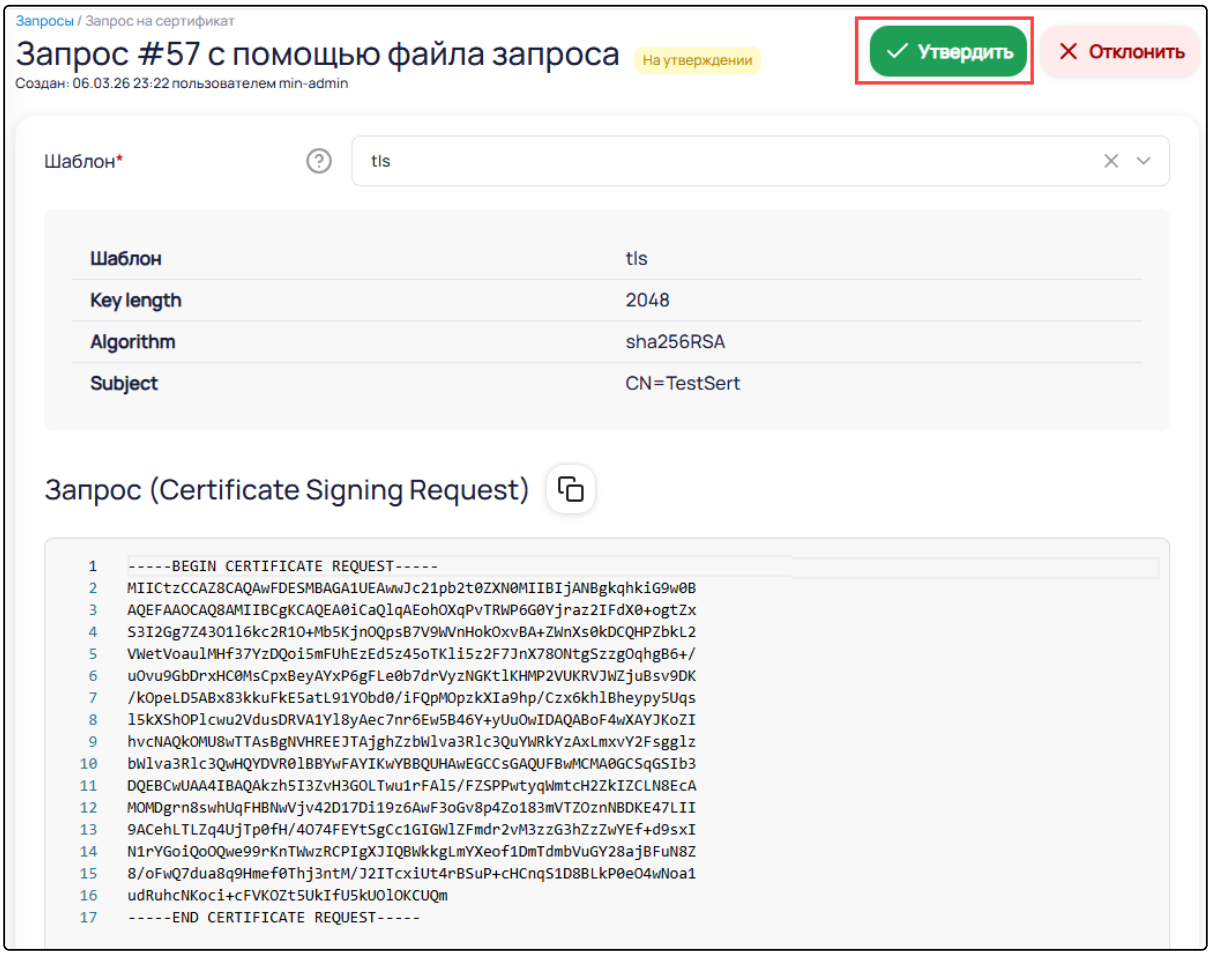
7. Запрос отправлен
   В правом верхнем углу появилось уведомление об успешном сохранении запроса, а новый запрос — в списке «Запросы» в статусе «Запросы».



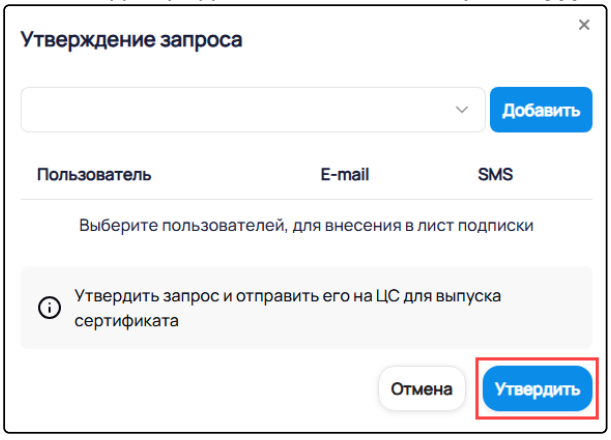
8. Откройте карточку запроса
   Нажмите на новый запрос в списке.



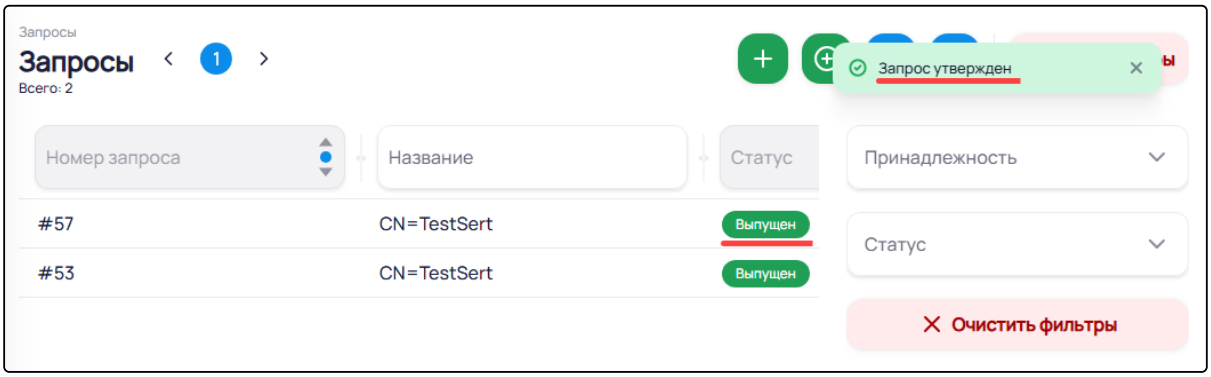
9. Утвердите запрос
   В открывшейся карточке нажмите кнопку **Утвердить**.



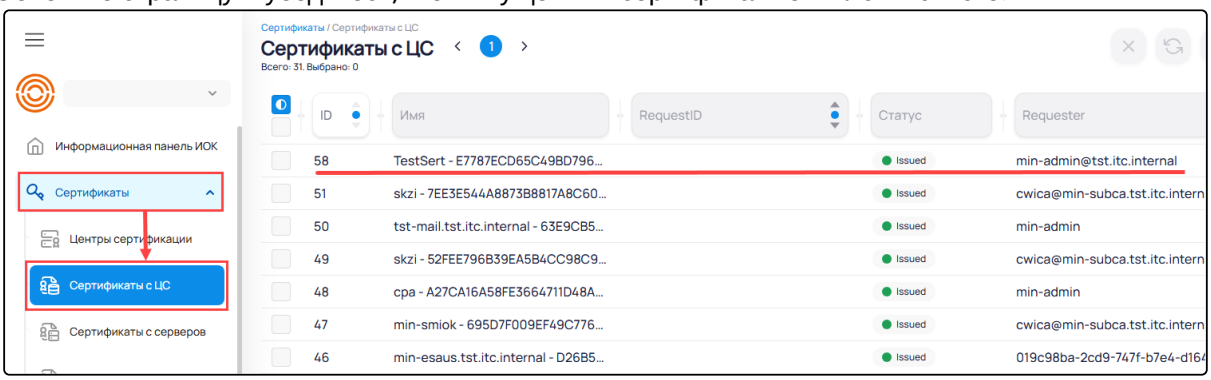
10. Подтвердите действие
    В окне подтверждения нажмите кнопку **Утвердить**.



11. Запрос утвержден
    В правом верхнем углу появилось уведомление об успешном утверждении запроса, а запрос сменил статус на «Выпущен»..



12. Дождитесь завершения выпуска сертификата
    Подождите 10 минут.
13. Проверьте список сертификатов
    Перейдите в раздел «Сертификаты» → подраздел «Сертификаты с ЦС».
    Обновите страницу и убедитесь, что выпущенный сертификат появился в списке.



4.5 Проверка статуса сервисов

Для проверки статуса сервисов запросите учетные данные администратора у сотрудников технической поддержки.

1. Авторизуйтесь по ssh:

```
ssh min-smiok.tst.itc.internal -l administrator
```

2. Перейдите в контекст пользователя:

```
sudo -su itc-svc
```

3. Проверьте статус работы сервисов командой:

```
systemctl list-units --user --type=service
```

4. Ожидаемый результат: отображает 22 запущенных сервиса со статусом Active: active (running). ПО запущено и функционирует.

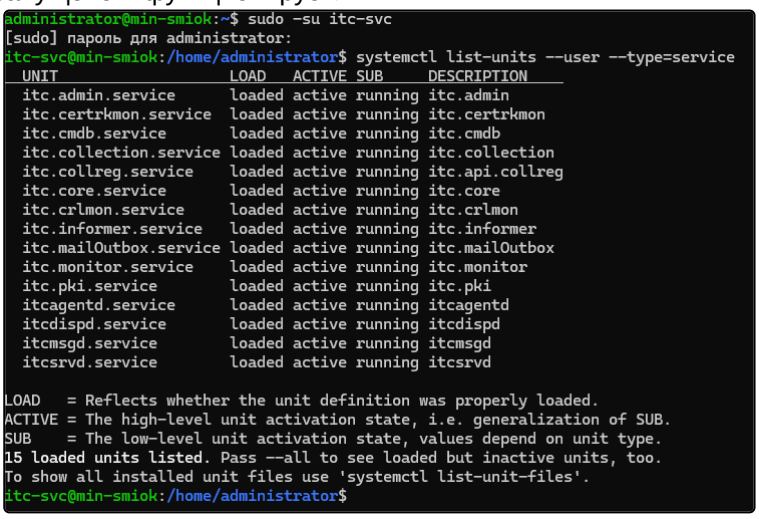


Рисунок 8 Запущенные службы СМИОК

5 Самостоятельная установка

5.1 Системные требования

Подробный набор требований для развертывания системы содержится в документе «Описание технической архитектуры программного обеспечения» в разделе «Физическая архитектура».

5.2 Инструкции по установке

Подробные инструкции для развертывания компонентов системы запросите у сотрудников технической поддержки.